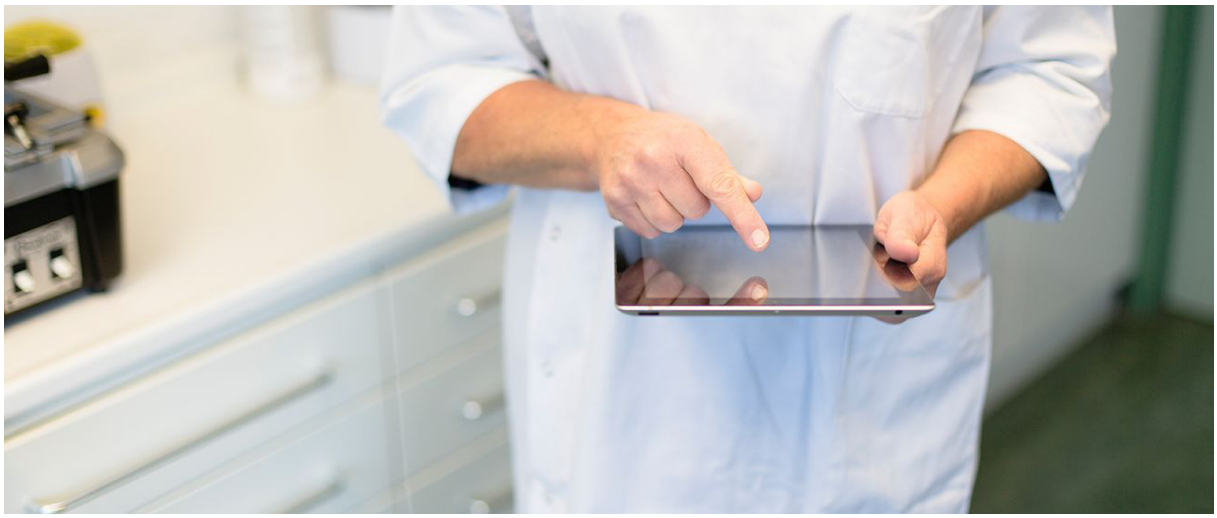
AUTORITEIT
PERSOONSGEGEVENS

Praktijkgids
Patiëntgegevens in de cloud



Nieuwe privacyregels vanaf 25 mei 2018

De informatie in deze praktijkgids is afgestemd op de huidige regels én op de nieuwe Europese regels van de Algemene verordening gegevensbescherming (AVG). Rond 25 mei 2018 gaan de nieuwe regels in. Dan vindt u in deze gids extra informatie.

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

Inhoudsopgave

1. Inleiding

Bent u zorgaanbieder en heeft u uw patiëntgegevens in de cloud[1] ondergebracht of overweegt u dit te doen? Dan kunt u deze praktijkgids gebruiken om dit op een verantwoorde manier te doen.

Deze gids biedt u namelijk een praktische invulling van de eerder door de Autoriteit Persoonsgegevens (AP) gepubliceerde beleidsregels *Beveiliging van persoonsgegevens*[2] voor de zorgaanbieder die zijn patiëntgegevens in de cloud bewaart of gaat bewaren.

De AP heeft deze praktijkgids gemaakt omdat patiëntgegevens bijzondere persoonsgegevens zijn, waarmee u zorgvuldig moet omgaan. Zulke gegevens zijn immers gevoeliger dan 'gewone' persoonsgegevens. Bovendien vallen patiëntgegevens onder het medisch beroepsgeheim van u als zorgaanbieder. Het gebruik van de cloud brengt daarnaast risico's met zich mee.

Het werken met patiëntgegevens in de cloud brengt de volgende risico's met zich mee:

- U merkt het mogelijk niet of pas te laat als informatie in verkeerde handen komt (datalek).
- Uw patiëntgegevens kunnen terechtkomen in een land waar de wettelijke bescherming van persoonsgegevens niet of onvoldoende is geregeld.
- De cloudprovider kan de gegevens voor zichzelf gebruiken zonder dat u hiervoor toestemming heeft gegeven.

De cloud kan voor u een goede oplossing zijn, maar is dus niet zonder gevaren. In deze praktijkgids leest u hoe u op een veilige manier in de cloud werkt.

De informatie in deze gids is afgestemd op de huidige regels én op de nieuwe Europese privacyregels die 25 mei 2018 ingaan (de Algemene verordening gegevensbescherming (AVG)). Rond de ingangsdatum van de nieuwe regels vindt u in deze praktijkgids extra informatie.

[1] Dit is bijvoorbeeld het geval indien u gebruikmaakt van Dropbox of Google Drive, en als de leverancier van uw patiëntinformatiesysteem (soms ook wel 'EPD' genoemd) niet alleen de software levert maar daarnaast ook de gegevensopslag verzorgt (en u de patiëntgegevens via een internetverbinding benadert). Zie ook de Begrippenlijst.
[2] Te downloaden via https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/thematische-beleidsregels/beleidsregels-beveiliging-van-persoonsgegevens-2013

2. Verantwoordelijke en bewerker

Als u uw patiëntgegevens in de cloud onderbrengt, bent u in de termen van de Wet bescherming persoonsgegevens (Wbp) de *verantwoordelijke* en is de cloudprovider de *bewerker*. Omdat het begrippenpaar verantwoordelijke/bewerker een belangrijke rol speelt in de verhouding tussen u en de cloudprovider, lichten we deze begrippen hieronder kort toe.

2.1 Verantwoordelijke

De *verantwoordelijke* in de zin van de Wbp is degene die 'het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'.[3] De verantwoordelijke bepaalt welke persoonsgegevens, voor welk doel, op welke manier en met welke middelen worden verwerkt.[4] In deze context bent u dat (zorgaanbieder).

2.2 Bewerker

Bij de verwerking van persoonsgegevens kan de verantwoordelijke een *bewerker*[5] inschakelen. De bewerker is 'een buiten de organisatie van de verantwoordelijke staande persoon of instelling'.[6] Hij 'bewerkt gegevens ten behoeve van de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid'.[7] De bewerker 'beperkt […] zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van persoonsgegevens. Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens enz.'[8]

2.3 Bewerkersovereenkomst

De rechtsverhouding tussen verantwoordelijke en bewerker wordt vastgelegd in een zogenoemde bewerkersovereenkomst. Hierin maken deze partijen afspraken over de verwerking van persoonsgegevens (zie verder onder 5.3 *Maak een bewerkersovereenkomst*).

2.4 Sub-bewerkers

Bij gebruik van de cloud wordt de dienstverlening soms uitgevoerd door een keten van bewerkers: de ingeschakelde bewerker maakt op zijn beurt weer gebruik van een derde partij om (een deel van de) persoonsgegevens te verwerken. Men spreekt dan van zogenaamde sub-bewerkers. U bent in zo'n geval verantwoordelijk voor de gehele keten van bewerkers.

De inschakeling van een subbewerker moet worden vermeld in de overeenkomst tussen de verantwoordelijke en de hoofdbewerker.

---

[3] artikel 1 sub d Wbp.
[4] De Europese toezichthouders op de gegevensbescherming hebben in 2010 een advies gepubliceerd over de begrippen 'verantwoordelijke' en 'bewerker', waarin deze beide begrippen uitgebreid en met voorbeelden worden toegelicht. *Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker'*, zie: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf
[5] artikel 1 sub e Wbp.
[6] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 61.
[7] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 61.
[8] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 61-62.

3. Waar moet u op letten als u overweegt uw patiëntgegevens in de cloud onder te brengen?

3.1 Geen toestemming nodig van de patiënt

U heeft geen toestemming van de patiënt nodig om uw patiëntgegevens in de cloud te plaatsen. De Wbp staat toe dat u ook zonder die toestemming uw gegevens laat verwerken door een bewerker.

Ook het medisch beroepsgeheim schrijft niet voor dat u hiervoor toestemming moet vragen. Artikel 7:457 Burgerlijk Wetboek (BW) bepaalt namelijk dat patiëntgegevens zonder toestemming mogen worden verstrekt aan 'degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst'. De AP beschouwt een cloudprovider die patiëntgegevens verwerkt voor de zorgaanbieder als 'rechtstreeks betrokken bij de uitvoering van de behandelingsovereenkomst'.

Volgens de Wet bescherming persoonsgegevens (Wbp) mag u patiëntgegevens in de cloud plaatsen zonder toestemming van uw patiënten. Ook het medisch beroepsgeheim schrijft niet voor dat u hiervoor toestemming moet vragen.

3.2 Speciale regels voor gebruik buitenlandse cloud

Als u uw gegevens onderbrengt bij een buitenlandse cloud, dan geldt dit als een 'doorgifte' in de zin van artikel 76 lid 1 Wbp. Voor doorgifte binnen de EU gelden geen bijzondere beperkingen. Voor doorgifte naar andere landen gelden wel speciale regels. Deze kunt u hier nalezen: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu

4. Hoe kiest u de juiste cloudprovider?

4.1 Voer eerst een risicoanalyse uit

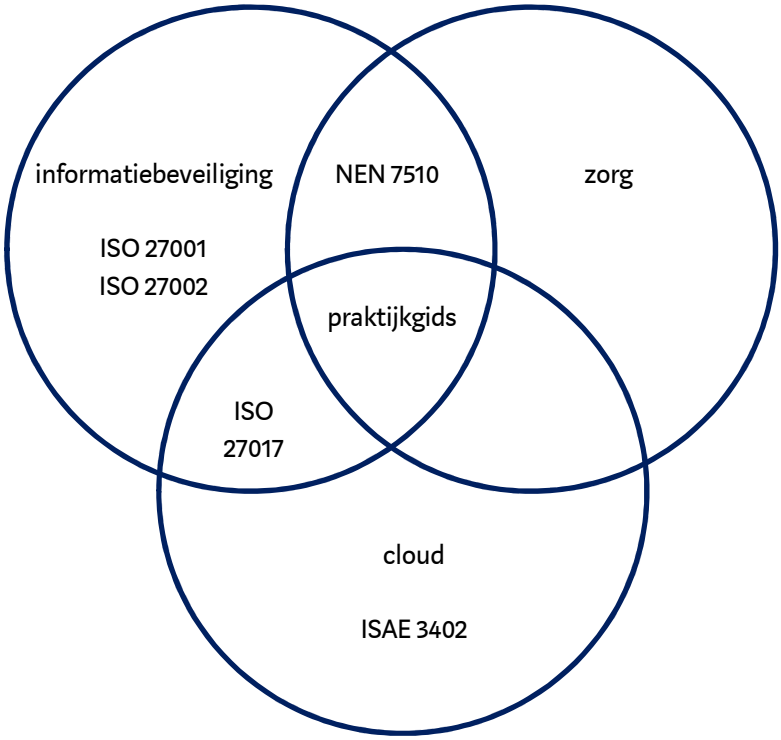
Voordat u in zee gaat met een cloudprovider moet u een risicoanalyse (laten) uitvoeren. Dan weet u welke risico's u loopt. Deze risicoanalyse moet regelmatig worden geactualiseerd. Lees meer over de risicoanalyse in de beleidsregels *Beveiliging van persoonsgegevens*, p. 29-32.

4.2 Controleer of de cloudprovider een certificaat heeft

Daarnaast kan een erkend certificaat zekerheid bieden over de kwaliteit van de cloudprovider. Zo'n certificaat bewijst namelijk dat de cloudprovider voldoet aan relevante praktijknormen.

Voor het gebruik van clouddiensten door zorgaanbieders bestaan verschillende normen. De meest relevante normen zijn ISAE 3402, ISO 27017 en NEN 7510. Daarnaast spelen ook de algemene beveiligingsnormen ISO 27001 en ISO 27002 een rol (zie hiervoor de beleidsregels *Beveiliging van persoonsgegevens,* p. 16).

Hoewel deze normen alle een eigen onderwerp bestrijken, is er ook sprake van overlap.
De werkingssfeer van deze normen wordt geïllustreerd in de volgende figuur.



Een certificaat is overigens niet verplicht.[9] Maar een certificaat toont wel aan dat de cloudprovider de in de betreffende norm voorgeschreven maatregelen heeft genomen. Dat geeft duidelijkheid voor u en eventueel ook voor de toezichthouder (AP).

4.3 Check of u altijd toegang houdt tot de gegevens

Overname of faillissement van de cloudprovider kan ertoe leiden dat de cloudprovider de dienstverlening aanpast. Het gevolg kan onder meer zijn dat de persoonsgegevens die de cloudprovider verwerkte tijdelijk of permanent niet meer voor u toegankelijk zijn. Ook wanprestatie door de cloudprovider is een risico voor de continuïteit van de dienstverlening. Om problemen te voorkomen zijn goede contractuele afspraken nodig (zie verder onder 5.3 *Maak een bewerkersovereenkomst*).

Het is daarnaast van groot belang dat u uw gegevens zonder al te veel rompslomp terug krijgt als u de samenwerking met de cloudprovider wilt beëindigen. Let erop dat cloudproviders niet altijd gebruik maken van standaarddatabasetechnologieën en -oplossingen. De bij hen aanwezige gegevens kunnen daardoor niet altijd zonder meer worden overgebracht naar een database van een andere bewerker of naar uw database. Dit is een belangrijk aandachtspunt bij de selectie van een cloudprovider.

Maak vooraf afspraken met de cloudprovider om ervoor te zorgen dat u toegang houdt tot de persoonsgegevens wanneer de provider wordt overgenomen of failliet gaat. Leg dat vast in een bewerkersovereenkomst.

[9] De betrouwbaarheid van een cloudprovider kan bijvoorbeeld ook blijken uit een auditrapport.

5. Hoe richt u de samenwerking met een cloudprovider goed in?

5.1 Zorg dat u aan de eisen van de Wbp voldoet

De Wbp stelt eisen aan de beveiliging van persoonsgegevens bij verwerking door een bewerker. Deze eisen zijn van toepassing op iedere vorm van verwerking door een bewerker, ook als de verwerking plaatsvindt in de cloud. Deze eisen zijn opgenomen in artikel 12 tot en met 14 Wbp. Concreet betekent dit voor de cloudprovider en voor u:

- De cloudprovider mag uw patiëntgegevens uitsluitend verwerken in opdracht van u.
- De cloudprovider mag zelf niets op eigen initiatief doen met die gegevens.
- De cloudprovider heeft een geheimhoudingsplicht.
- U moet ervoor zorgen dat de cloudprovider uw patiëntgegevens goed beveiligt.

5.2 Volg de aanvullende eisen uit de beleidsregels *Beveiliging van persoonsgegevens*

In hoofdstuk 3 van de beleidsregels *Beveiliging van persoonsgegevens* geeft de AP aan hoe zij de beveiliging van persoonsgegevens in het algemeen beoordeelt. Hoofdstuk 4 bevat vervolgens de specifieke uitgangspunten voor verwerking door een bewerker. Beide hoofdstukken moeten in samenhang worden gelezen.

Houdt u er in elk geval rekening mee dat het hoogste beveiligingsniveau is vereist voor gegevens waarop het medisch beroepsgeheim van toepassing is.[10] Dat betekent in elk geval dat u:

- de gegevens moet versleutelen, zowel *in transit* (onderweg van cloud naar gebruiker of vice versa) als *at rest* (in opslag);
- voor hoogwaardige autorisatie- en authenticatiemechanismen moet zorgen;
- moet checken of uw data volledig zijn afgezonderd van de data van andere klanten van uw cloudprovider.

5.3 Maak een bewerkersovereenkomst

U bent verplicht een schriftelijke bewerkersovereenkomst te sluiten met uw cloudprovider(artikel 14 lid 2 en artikel 14 lid 5 Wbp). Daarin legt u alle afspraken vast die u met de cloudprovider heeft gemaakt. In de beleidsregels *Beveiliging van persoonsgegevens* (p. 32-34) leest u welke eisen de AP stelt aan zo'n overeenkomst.

In de Wbp en de beleidsregels *Beveiliging van persoonsgegevens* staan de eisen en uitgangspunten waar bewerkers aan moeten voldoen. Dat helpt u om de samenwerking met de cloudprovider goed in te richten.

[10] *Beveiliging van persoonsgegevens*, p. 20.

6. Waar moet u verder nog op letten als de gegevens eenmaal in de cloud zitten?

6.1 Houd toezicht op de cloudprovider

U moet regelmatig controleren of de cloudprovider de afspraken in de bewerkersovereenkomst naleeft. En of de cloudprovider de vereiste technische en organisatorische beveiligingsmaatregelen daadwerkelijk heeft genomen (zie verder *Beveiliging van persoonsgegevens*, p. 34-35).

6.2 Evalueer en pas zo nodig aan

Daarnaast evalueert u periodiek de bewerking door de cloudprovider. Als zich tussentijds grote veranderingen voordoen, beoordeelt u deze en voert u eventuele aanpassingen door (zie verder *Beveiliging van persoonsgegevens*, p. 35-36). Het kan nodig zijn dat u nieuwe afspraken met de cloudprovider maakt. Soms kan de evaluatie er zelfs toe leiden dat u met een andere cloudprovider verder gaat.

6.3 Wat te doen bij een datalek?

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat u direct een melding moet doen bij de AP zodra u een ernstig datalek heeft. En soms moet u het datalek ook melden aan uw patiënten.

Hier leest u in welke situaties en hoe u een datalek meldt bij de AP:
https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken.

U kunt afspreken met de cloudprovider - bijvoorbeeld in de bewerkersovereenkomst - dat die namens u datalekken meldt.

Zie voor beide situaties verder de *Beleidsregels meldplicht datalekken*, hoofdstuk 2:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

Let op !

Vanaf 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Het is nog niet duidelijk of een bewerker volgens deze nieuwe Europese regels het datalek mag melden of dat u dit als verantwoordelijke zelf moet doen.

Doet u de meldingen zelf? Dan moet u ervoor zorgen dat u tijdig weet dat er een datalek is. Spreek daarom met de bewerker af dat die u onmiddellijk op de hoogte stelt van eventuele datalekken. U doet dit bij voorkeur door het in de bewerkersovereenkomst op te nemen.

Let op !

Wanneer de nieuwe Europese privacyregels ingaan, is een bewerker verplicht om een datalek direct aan u als verantwoordelijke te melden. U hoeft hierover dan geen aparte afspraken meer te maken.

7. Wat zijn de consequenties als u niet aan de regels voldoet?

Als u zich niet houdt aan de voorschriften van de Wbp, dan krijgt u te maken met de toezichthouder AP. Zo kan de AP u dwingen de overtreding ongedaan te maken (last onder bestuursdwang; artikel 65 Wbp). Ook kan de AP u een bestuurlijke boete opleggen (artikel 66 Wbp) van maximaal € 820.000.

Let op !

Onder de nieuwe Europese privacyregels kan de AP u een boete opleggen van maximaal 20 miljoen euro of 4 procent van de totale wereldwijde jaaromzet.

8. Begrippenlijst

Bijzondere persoonsgegevens
Gegevens als bedoeld in artikel 16 Wbp. Verwerking van deze gegevens is slechts beperkt toegestaan.

Cloud
Een gedeelde verzameling configureerbare computermiddelen (zoals netwerken, servers, opslag, toepassingen en diensten), toegankelijk via internet.

Cloudprovider
Aanbieder van clouddiensten.

Datalek
Inbreuk op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 Wbp): toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is. Onder een datalek valt niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens, zoals toegang door onbevoegden.

Medisch beroepsgeheim
Geheimhoudingsplicht voor mensen die vanwege hun beroep met medische gegevens werken. Zij mogen in principe geen gegevens van een patiënt aan anderen verstrekken. Voor zorgverleners zoals artsen, verpleegkundigen, psychotherapeuten en andere beroepen die vallen onder de Wet Beroepen in de Individuele Gezondheidszorg (BIG) geldt het wettelijk geregeld medisch beroepsgeheim (artikel 88 Wet BIG en in geval van een geneeskundige behandelingsovereenkomst ook artikel 7:457 BW). Voor sommige andere hulpverleners, zoals maatschappelijk werkers, geldt een geheimhoudingsplicht op grond van hun beroepscode. De medewerkers van de zorginstelling (zoals een ziekenhuis) waar iemand een behandeling ondergaat, zijn via hun arbeidscontract aan een geheimhoudingsplicht gebonden.

Patiëntgegevens
De gegevens opgenomen in het dossier als bedoeld in artikel 7:454 lid 1 BW.

Zorgaanbieder
Zorginstelling, zorgpraktijk of een zelfstandig werkende individuele zorgverlener (zie ook artikel 1 Wet kwaliteit, klachten en geschillen zorg).

9. Wetteksten

Wet bescherming persoonsgegevens

Artikel 1 sub d
Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Artikel 1 sub e
Bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Artikel 12
Lid 1 Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen.

Lid 2 De personen, bedoeld in het eerste lid, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit. Artikel 272, tweede lid, van het Wetboek van Strafrecht is niet van toepassing.

Artikel 13
De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 14
Lid 1 Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen, en ten aanzien van de melding van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt. De verantwoordelijke ziet toe op de naleving van die maatregelen.

Lid 2 De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.

Lid 3 De verantwoordelijke draagt zorg dat de bewerker:
a. de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid;
b. de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13, en
c. de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplichting tot melding van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt.

Lid 4 Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b en c.

Lid 5 Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, de beveiligingsmaatregelen, bedoeld in artikel 13, en de verplichting tot melding van een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt, schriftelijk of in een andere, gelijkwaardige vorm vastgelegd.

Artikel 16
De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf. Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Burgerlijk Wetboek

Artikel 7:454 lid 1
De hulpverlener richt een dossier in met betrekking tot de behandeling van de patiënt. Hij houdt in het dossier aantekening van de gegevens omtrent de gezondheid van de patiënt en de te diens aanzien uitgevoerde verrichtingen en neemt andere stukken, bevattende zodanige gegevens, daarin op, een en ander voor zover dit voor een goede hulpverlening aan hem noodzakelijk is.

Artikel 7:457
Lid 1 Onverminderd het in artikel 448 lid 3, tweede volzin, bepaalde draagt de hulpverlener zorg, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden, bedoeld in artikel 454, worden verstrekt dan met toestemming van de patiënt. Indien verstrekking plaatsvindt, geschiedt deze slechts voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. De verstrekking kan geschieden zonder inachtneming van de

beperkingen, bedoeld in de voorgaande volzinnen, indien het bij of krachtens de wet bepaalde daartoe verplicht.

Lid 2 Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden.

Lid 3 Daaronder zijn evenmin begrepen degenen wier toestemming ter zake van de uitvoering van de behandelingsovereenkomst op grond van de artikelen 450 en 465 is vereist. Indien de hulpverlener door inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden te verstrekken niet geacht kan worden de zorg van een goed hulpverlener in acht te nemen, laat hij zulks achterwege.

Wet Beroepen in de Individuele Gezondheidszorg

Artikel 88
Een ieder is verplicht geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim te zijner kennis is gekomen of wat daarbij te zijner kennis is gekomen en waarvan hij het vertrouwelijke karakter moest begrijpen.

10. Praktijknormen cloud en beveiliging

10.1 ISAE 3402

De ISAE 3402-standaard bevat richtlijnen voor het afgeven van een zogenaamde 'third party mededeling' (TPM). Een TPM is een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de maatregelen die de bewerker heeft getroffen. De TPM wordt opgesteld in opdracht van de bewerker, en wordt verstrekt aan de verantwoordelijken die gebruik maken van de diensten van de bewerker. Op die manier krijgen verantwoordelijken inzicht in de getroffen maatregelen, zonder dat iedere verantwoordelijke daarnaar zelf onderzoek hoeft te (laten) doen.

Binnen ISAE 3402 is de basis voor de TPM een beschrijving door de bewerker van de maatregelen die voor de doelgroep van de TPM relevant zijn. De externe deskundige toetst deze beschrijving onder meer op volledigheid en stelt vervolgens vast of de bewerker de beschreven maatregelen daadwerkelijk heeft getroffen. Afhankelijk van het type TPM doet de externe deskundige een uitspraak over de aanwezigheid van de beschreven maatregelen op een bepaalde datum (type 1) of gedurende een bepaalde periode (type 2).

Een TPM kan een goed middel zijn om vast te stellen of de cloudprovider de noodzakelijke organisatorische en technische beveiligingsmaatregelen daadwerkelijk getroffen heeft.

10.2 ISO/IEC 27017:2015

De ISO/IEC 27017:2015- norm geeft, uitgaande van ISO/SEC 27002, richtlijnen voor informatiebeveiliging bij het gebruik van clouddiensten. Certificering voor de ISO/IEC 27017:2015-norm is mogelijk in combinatie met ISO/IEC 27001.

ISO/IEC 27001
(Nederlandse versie NEN-ISO/IEC 27001nl)

Deze standaard bevat eisen waar het managementsysteem voor informatiebeveiliging aan dient te voldoen. Met de standaard kunnen leveranciers aantonen dat zij aan de vereiste informatiebeveiligingsnormen voldoen. Bij certificering wordt ook tegen deze norm ge-audit.

De standaard specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's van een organisatie. Het ISMS, het managementsysteem voor informatiebeveiliging, is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatievoorziening beveiligen.

ISO/SEC 27002
(Nederlandse versie NEN-ISO/IEC 27002nl)

Deze standaard is een 'best practice' van beveiligingsmaatregelen ('controls') om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en

beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van de NEN-ISO/IEC 27001.

ISO 27002 *Code voor informatiebeveiliging* geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid.

10.3 NEN 7510

NEN 7510 is een Nederlandse, sectorspecifieke uitwerking van ISO/SEC 27002 voor de zorg. NEN 7510 verwijst naar ISO/IEC 27001 voor het bijbehorende managementsysteem. In paragraaf 6.2 van de NEN 7510-norm wordt bijzondere aandacht besteed aan het beveiligen van informatie die externe partijen verwerken of beheren. Sinds 2016 kan geaccrediteerde certificering plaatsvinden op basis van NEN 7510.[11]

[11] Zie https://www.nen.nl/Normontwikkeling/Certificaten/Schemabeheer/Zorg-en-Welzijn-NEN-7510.htm

11. Contactgegevens

Bezoekadres
(alleen volgens afspraak)
Bezuidenhoutseweg 30
2594 AV DEN HAAG

Let op: bij bezoek aan de Autoriteit Persoonsgegevens moet u een geldig identiteitsbewijs laten zien.

Postadres
Postbus 93374
2509 AJ DEN HAAG
www.autoriteitpersoonsgegevens.nl

Telefonisch spreekuur
Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de bescherming van persoonsgegevens. Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met de publieksvoorlichters van de Autoriteit Persoonsgegevens tijdens het telefonisch spreekuur via telefoonnummer **0900-2001 201**. Tariefinformatie vindt u op onze website op de pagina telefonisch contact. De publieksvoorlichters zijn bereikbaar op maandag, dinsdag, donderdag en vrijdag van 10.00 tot 12.00 uur.

Persvoorlichting
Journalisten en redacteuren kunnen met vragen terecht bij de woordvoerders van de Autoriteit Persoonsgegevens via telefoonnummer **070-8888 555**.

Zakelijke relaties
Bent u een zakelijke relatie van de Autoriteit Persoonsgegevens, zoals een leverancier, dan kunt u ons telefonisch bereiken via telefoonnummer **070-8888 500**.