Is uw praktijk klaar voor de AVG?

Doe de check!

infomedics

Vanaf 25 mei 2018 is het nóg belangrijker geworden om de bescherming van persoonsgegevens als eerstelijns zorgpraktijk goed op orde te hebben. Op die dag is de Algemene Verordening Gegevensbescherming (AVG) - de nieuwe Europese privacywetgeving - van kracht geworden. In deze whitepaper leest u waarom dataveiligheid en het zorgdragen voor de privacy van uw patiënten en cliënten zo ontzettend belangrijk is.

Verder ontdekt u wat er allemaal is veranderd onder de nieuwe wetgeving en wat dat voor uw praktijk betekent. Tot slot vindt u in deze whitepaper een handige checklist. Daarmee ziet u snel of uw praktijk klaar is voor de nieuwe privacywet én ontdekt u of u veilig omgaat met de (data)privacy van patiënten en cliënten.

1 Datazorgplicht

Waarom is privacy & dataveiligheid zo belangrijk?

Waarom is het beveiligen van patiëntendata zo belangrijk? U hebt vast gehoord dat de Autoriteit Persoonsgegevens het recht heeft om boetes uit te delen wanneer bedrijven zich niet aan de wet houden. Wie nalatig is kan op stevige sancties rekenen. Onder de AVG is de bevoegdheid van de Autoriteit Persoonsgegevens verruimd tot boetes van 4% van de jaaromzet van de overtreder tot een maximum van 20 miljoen euro.

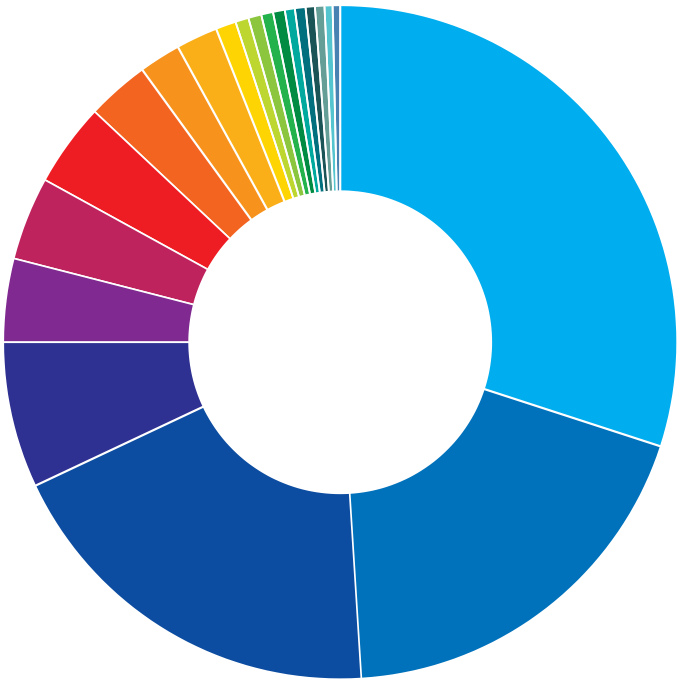
Zorgplicht betekent óók datazorgplicht

Vanaf 25 mei loopt u dus een behoorlijk financieel risico wanneer u zich niet aan de wet houdt. Maar dat zou niet de reden moeten zijn om de dataveiligheid in uw praktijk op orde te brengen. Waarom dan wel? Het is simpelweg onderdeel van uw zorgplicht. Als zorgverlener draagt u niet alleen zorg voor het gebit of de geestelijke gezondheid van uw patiënt, maar ook voor de veiligheid van diens gegevens.

Medisch Nederland is zo lek als een mandje

Dat er nog veel winst te behalen is, blijkt uit *een rapport van de Autoriteit Persoonsgegevens over datalekken in 2017.* Vorig jaar zijn er ruim 10.000 lekken gemeld, waarvan 30% in de sector Gezondheid en Welzijn. De zorgsector staat daarmee met stip op nummer 1 als het om datalekken gaat. Geen positie om trots op te zijn.

Bovendien is het nog maar de vraag of deze cijfers realistisch zijn. Vaak zijn zorgverleners zich niet eens bewust van veroorzaakte datalekken. Soms is het niet duidelijk dat er sprake is van een datalek. En als dat wel het geval is, wordt er lang niet altijd melding van gemaakt bij de Autoriteit Persoonsgegevens.



Bron: Meldplicht datalekken: facts & figures (2017), Autoriteit Persoonsgegevens

Gezondheid en welzijn	30%	Energie	1%
Openbaar bestuur	19%	Onroerend goed	1%
Financiële dienstverlening	19%	Bouw	<1%
Informatie en communicatie	7%	Industrie	<1%
Overige organisaties	4%	Cultuur, sport en recreatie	<1%
Vervoer	4%	Landbouw, bosbouw en visserij	<1%
Overige zakelijke dienstverlening	4%	Horeca	<1%
Onderwijs	3%	Water en milieu	<1%
Specialistische zakelijke dienstverlening	2%	Extraterritoriale organisaties en lichamen	0%
Politie en justitie	2%	Mijnbouw	0%
Handel en autobranche	1%		

Patiëntendata is veel geld waard

De persoonsgegevens die u verzamelt zijn veel geld waard voor hackers. Met de combinatie van persoonsgegevens die een eerstelijns zorgpraktijk bewaart (NAW gegevens, BSN en medische gegevens) kan een hacker identiteitsfraude plegen. Denk aan vakanties bestellen, een abonnement afsluiten, een nieuw DigiD aanvragen en ga zo maar door.

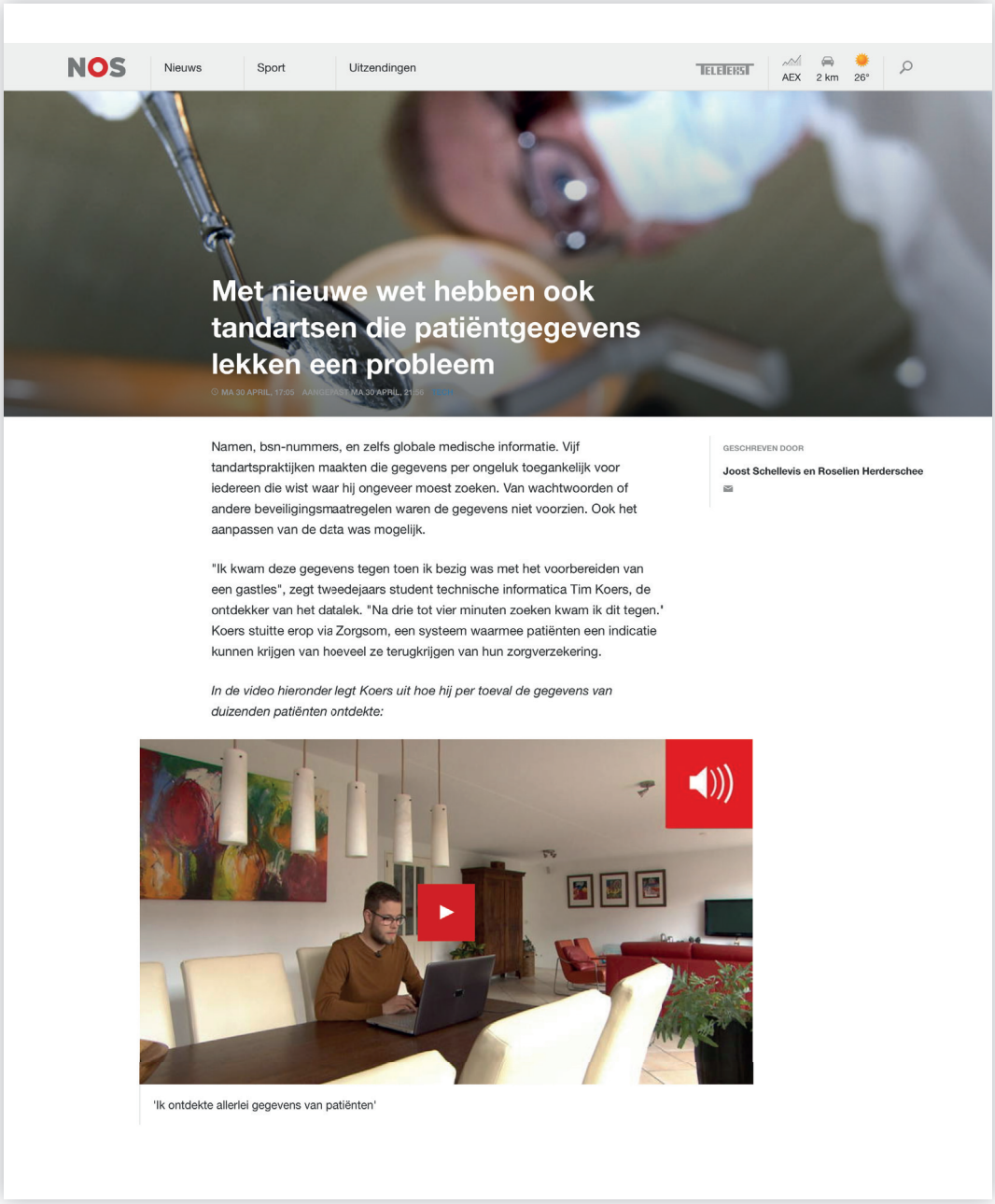
Een dataset van één patiënt levert al snel een paar honderd euro op. Stel, een hacker kan 200 euro per dataset vragen op de zwarte markt. Wanneer er 4.000 patiënten staan ingeschreven in uw praktijk, vertegenwoordigen de gegevens waar u verantwoordelijk voor bent een waarde van zo'n 800.000 euro. Dat is een aantrekkelijke buit!

Eerstelijns zorgpraktijken zijn doelwit van internetcriminelen

Eerstelijns zorgpraktijken zijn dan ook steeds vaker doelwit van internetcriminelen. Uit onderzoek van Qfast uit 2016 blijkt dat er bij het totaal van de 26 praktijken in het forensisch onderzoek maar liefst 6 miljoen aanvallen op maandbasis plaatsvonden. Uit datzelfde onderzoek blijkt dat de technische beveiliging vaak onder de maat is, dat software niet up-to-date is, dat ICT slecht en ad hoc wordt beheerd en dat er veel menselijke fouten worden gemaakt.

Werkstations achter de balie van een tandartspraktijk zijn bijvoorbeeld vaak onbeheerd. De receptiemedewerker loopt ‘even weg’ en vergrendelt het werkstation niet. Vervolgens kan iedere onwelwillende met een USB-stick in enkele seconden software installeren. Die software kan wachtwoorden opslaan en hackers van buitenaf toegang geven tot de pc en zelfs tot dataservers.
Los van de financiële risico’s die u loopt wanneer een hacker patiëntgegevens buitmaakt, loopt uw imago een flinke deuk op. Patiënten worden zich immers steeds meer bewust van de risico’s. Met regelmaat verschijnen berichten in de media die laten zien waar het misging.

Bron: nu.nl: Datalek Nijmeegse tandartsenprakijk (29 december 2017)



NOS Nieuws Sport Uitzendingen TELETEKST AEX 2 km 26°

Met nieuwe wet hebben ook tandartsen die patiëntgegevens lekken een probleem

MA 30 APRIL, 17:05 AANGEPAST MA 30 APRIL, 21:56

GESCHREVEN DOOR

Joost Schellevis en Roselien Herderschee

Namen, bsn-nummers, en zelfs globale medische informatie. Vijf tandartspraktijken maakten die gegevens per ongeluk toegankelijk voor iedereen die wist waar hij ongeveer moest zoeken. Van wachtwoorden of andere beveiligingsmaatregelen waren de gegevens niet voorzien. Ook het aanpassen van de data was mogelijk.

"Ik kwam deze gegevens tegen toen ik bezig was met het voorbereiden van een gastles", zegt tweedejaars student technische informatica Tim Koers, de ontdekker van het datalek. "Na drie tot vier minuten zoeken kwam ik dit tegen." Koers stuitte erop via Zorgsom, een systeem waarmee patiënten een indicatie kunnen krijgen van hoeveel ze terugkrijgen van hun zorgverzekering.

In de video hieronder legt Koers uit hoe hij per toeval de gegevens van duizenden patiënten ontdekte:

'Ik ontdekte allerlei gegevens van patiënten'

Bron: nos.nl (1 mei 2018)

2 Welke veranderingen brengt de AVG?

Belangrijke gevolgen voor de eerstelijns zorgpraktijk

Dataveiligheid en privacy zijn dus ontzéttend belangrijk. Veel zaken waar uw zorgpraktijk aan moet voldoen om dataveiligheid te waarborgen, waren al geregeld in de vorige wet; de Wet Bescherming Persoonsgegevens. De komst van de AVG zet ons op scherp, en dat is alleen maar goed. Wat is er per 25 mei veranderd? En welke gevolgen heeft deze nieuwe wet voor uw praktijk?

Meer rechten en meer verantwoordelijkheden

Zeggen dat u patiëntgegevens goed beschermt, is voor de AVG niet langer genoeg. U moet ook kunnen aantonen hoe u dat doet.

De AVG brengt daarnaast twee grote veranderingen met zich mee:

1. De rechten van patiënten worden uitgebreid

Patiënten (in de AVG 'betrokkenen' genoemd) hebben onder de AVG *meer rechten gekregen*, als het gaat om hun persoonlijke data. Betrokkenen hebben bijvoorbeeld het *recht op vergetelheid* (of verwijdering). Dat wil zeggen; een patiënt moet een verzoek kunnen indienen om zijn of haar data te laten verwijderen, natuurlijk met inachtneming van de wettelijke bewaartermijnen.

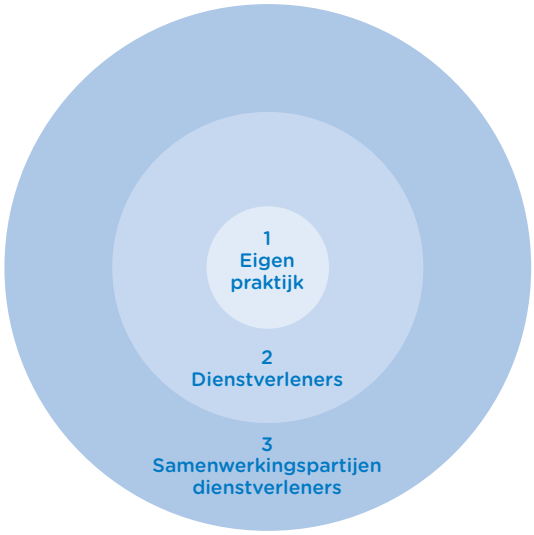
Daarnaast is het recht op *dataportabiliteit* (het kunnen meenemen van eigen gegevens) toegevoegd. Verder heeft de patiënt o.a. het recht op *rectificatie en aanvulling* (om gegevens te kunnen wijzigen), op *beperking van de verwerking* (om minder gegevens te laten verwerken) en het recht *om bezwaar te maken.*

2. De zorgpraktijk krijgt veel meer verantwoordelijkheden

Partijen die persoonsgegevens verwerken, krijgen onder de AVG meer verantwoordelijkheden. Ten eerste moet u als zorgpraktijk uw systemen, processen en interne organisatie zo aanpassen, dat u vanaf 25 mei *op de juiste manier gehoor kunt geven aan verzoeken* van patiënten die betrekking hebben op de hierboven genoemde rechten.

Betrokkenen hebben bovendien recht op duidelijke informatie over wat u met hun persoonsgegevens doet. Onder de AVG moet u daarvoor aan specifieke eisen voldoen, waaronder het opstellen van een privacyverklaring, een intern privacybeleid, verwerkersovereenkomsten met partijen die voor u gegevens verwerken en ga zo maar door. Meer daarover leest u in het volgende hoofdstuk.

Dataveiligheid heeft betrekking op drie kringen



Als zorgpraktijk is het dus zaak om goed zorg te dragen voor de data van patiënten die u verzamelt en verwerkt. Dat gaat echter verder dan alleen uw eigen gedragingen. Dataveiligheid heeft namelijk betrekking op drie kringen.

KRING 1: de eigen praktijk

De eerste kring is de eigen praktijk; hoe u zelf met data en privacy omgaat. Hier hebt u veel invloed op. De tips en checklist in deze whitepaper helpen u op weg om dit op een goede manier te organiseren.

KRING 2: dienstverleners met wie u data deelt

De tweede kring heeft betrekking op partijen met wie u patiëntendata deelt. Dat kan bijvoorbeeld uw webhost zijn, de leverancier van praktijksoftware, maar ook het administratiekantoor of de factoringmaatschappij die facturen voor u verstuurt. Ga na hoe zij alles geregeld hebben. Werken ze AVG-proof? Zijn ze ISO27001-gecertificeerd? Gebruiken ze tweestapsverificatie wanneer ze uw patiënten toegang geven tot hun persoonlijke en betaalgegevens? En hoe gaan zij om met eventuele datalekken?

KRING 3: bedrijven die samenwerken met uw dienstverleners

De derde kring bevat de bedrijven die samenwerken met de dienstverleners die u inschakelt. Verzorgen wij, Infomedics, het debiteurenbeheer voor uw praktijk, dan is het goed om te weten dat we de patiëntdata delen met zorgvuldig geselecteerde partijen. We verwerken gemiddeld bijna 300.000 rekeningen per week. Het printen, vouwen, in een envelop stoppen en verzenden van alle rekeningen aan patiënten besteden we uit aan een printservice.

Omdat dataveiligheid voor ons ontzettend belangrijk is, is deze printspecialist - net als wij - ISO27001-gecertificeerd. U kunt er dus vanuit gaan dat ook deze derde partij zorgvuldig met de patiëntdata omgaat. Kortom; ga na of ook partijen in de derde kring AVG-proof werken en zorgvuldig omgaan met de patiëntdata waar u verantwoordelijk voor bent.

3 Werkt uw praktijk AVG & privacy proof?

Doe de check!

Wat kunt u doen om privacy proof te werken? Hieronder leest u welke stappen u moet zetten om informatieveiligheid en privacy hoog op de agenda te zetten en om te voldoen aan de nieuwe wetgeving. Deze stappen zijn verdeeld over vier categorieën; bewustzijn & gedrag, hardware & software, AVG-eisen & documentatie en tot slot processen & facturatie. Na dit hoofdstuk vindt u een handige samenvatting in de vorm van een checklist.

Eerst nog even een disclaimer

Deze checklist is opgesteld om u te helpen bewuster om te gaan met informatieveiligheid en privacy. Deze whitepaper is echter geen juridisch document en de checklist is niet uitputtend. Om onduidelijkheid te voorkomen; u kunt er geen rechten aan ontlenen. Zie het als een richtlijn, een hulpmiddel.
Als u onderstaande zaken goed regelt, bent u een heel eind op weg. Wilt u zeker weten dat u goed zit? Schakel dan een jurist en/of specialist in op het gebied van informatiebeveiliging.

1. Bewustzijn & Gedrag

Informatieveiligheid begint bij het creëren van bewustzijn binnen het team. Vaak wordt er nog te laconiek gedaan over privacy en informatieveiligheid en zijn de risico's niet bekend. Investeer daarom in training en bewustwording.

Wat u sowieso NIET (meer) moet doen:

- ➜ Werkstations onbemand en niet gelockt achterlaten.
- ➜ Patiëntengegevens bespreken waar andere mensen bij zijn.
- ➜ Wachtwoorden nooit veranderen of op post-its of onder toetsenborden laten rondslingeren.
- ➜ Patiëntgegevens via de mail uitwisselen.
- ➜ De mappenkast met patiëntendossiers niet afsluiten.
- ➜ Zaken op de bureaus laten slingeren na werktijd.

Wat WEL verstandig is om te doen:

- ➜ Een periodiek overleg organiseren met alle medewerkers, waarin informatieveiligheid en privacy uitgebreid worden besproken. Ga regelmatig na of de bestaande maatregelen nog afdoende zijn en inventariseer of er nog risico's bij zijn gekomen.
- ➜ Uw ICT-omgeving zorgvuldig inrichten en beveiligen. Doe dit niet zelf, maar schakel hier een ICT-specialist voor in.
- ➜ Er voor zorgen dat medewerkers beveiligingsincidenten melden. Vermoedt u dat er een datalek is, of hebt u er één geconstateerd, dan bent u verplicht dit door te geven aan de Autoriteit Persoonsgegevens. *Dat kan eenvoudig via de website van de Autoriteit Persoonsgegevens.*
- ➜ Regelmatig wachtwoorden veranderen en medewerkers trainen op het gebruik van veilige wachtwoorden.
- ➜ Computers altijd vergrendelen wanneer u van uw werkplek wegloopt.
- ➜ Een clean desk policy invoeren en strikt naleven.

2. Hardware & Software

Waar slaat u patiëntgegevens op? Is dat op een plek waar iedereen bij kan? Of staat de server achter slot en grendel? En hoe zit het met de computers, laptops en telefoons die collega's gebruiken om patiëntgegevens te bekijken en verwerken? Ook de software die u gebruikt moet AVG-proof zijn.

Wat u moet regelen:

- ➜ Zorg dat *computers onbereikbaar* zijn voor derden en dat er geen patiënten bij kunnen.
- ➜ U bent verplicht om gegevens een aantal jaren te bewaren, maar doe dit op een veilige manier. *Bewaar niet alle informatie op één pc,* maar trek het liever uit elkaar. Sla bijvoorbeeld NAW-gegevens en informatie over behandelingen op twee verschillende plekken op. Zo is het voor hackers moeilijker om een compleet dataprofiel per patiënt te stelen. Zorg er sowieso voor dat alle data *encrypted* (versleuteld) is.
- ➜ Check of de *praktijksoftware* (zoals Exquise, Novadent of Simplex) die u gebruikt voldoet aan de eisen van de AVG. Zorg ook voor een verwerkersovereenkomst met deze partij (zie AVG: Eisen & Documentatie).
- ➜ Ga na of de patiëntenportalen die u of uw leveranciers inzetten, gebruik maken van de nodige beveiligingsmaatregelen.
  Een goed patiëntenportaal is beveiligd via tweestapsverificatie. Behalve een gebruikersnaam en een wachtwoord, heeft de gebruiker dan een via SMS of e-mail ontvangen code nodig om in te loggen.
- ➜ Kies software *van leveranciers uit de EU:* dan weet u zeker dat ze aan de AVG moeten voldoen.
- ➜ Zorg dat u geen gevoelige data opslaat op *Google Drive of Dropbox.* Deze partijen slaan data op in de VS, en dat betekent dat ze niet onder de AVG, maar onder de Amerikaanse wetgeving vallen. De moraal en regels ten aanzien van privacy zijn in de VS heel anders dan hier.
- ➜ Werken collega's soms thuis of onderweg? Zorg dat de hardware die ze gebruiken veilig is en zorg ook voor *een veilige verbinding.* Dat kan met VPN (Virtual Private Network) of met een dongel.

3. AVG: Eisen & Documentatie

Vanaf 25 mei moet u aan een aantal eisen voldoen. Daarnaast bent u verplicht om een aantal documenten op te stellen en op de juiste plek aan te bieden. Dit zijn de belangrijkste zaken die u moet regelen:

- *Privacyverklaring.* Volgens de AVG moet u patiënten duidelijk informeren over wat u met hun persoonsgegevens doet. U kunt hiervoor een privacyverklaring gebruiken. Daarin vermeldt u welke gegevens u verzamelt, hoe u die opslaat, hoe lang u ze bewaart, met wie u ze deelt en waarom. Daarnaast kunt u in de privacyverklaring opnemen op welke manier patiënten gebruik kunnen maken van hun rechten (zoals vergetelheid en dataportabiliteit). De beste manier om er zeker van te zijn dat patiënten uw privacyverklaring kunnen vinden, is deze te publiceren op uw website.
- *Verwerkersovereenkomst.* U bent verantwoordelijk voor de patiëntdata die u verzamelt. Maar vaak bent u niet de enige die deze data verwerkt. U bent verplicht om met iedere verwerker een verwerkersovereenkomst af te sluiten. Vaak stelt de verwerker zo'n overeenkomst voor u op. Is dat niet zo, dan moet u hier zelf zorg voor dragen.
- *Intern privacybeleid.* Een intern privacybeleid beschrijft hoe uw praktijk met de beveiliging van informatie omgaat. Het is bedoeld voor alle medewerkers en vertelt hoe ze in de dagelijkse gang van zaken moeten omgaan met persoonsgegevens en privacybescherming. Bewustzijn en professioneel handelen van uw medewerkers helpen bij het voorkomen van een datalek.
- *Verwerkingsregister.* In een verwerkingsregister houdt u bij waar in uw systemen persoonsgegevens worden verwerkt. Als u persoonsgegevens met derden deelt, dan moet u dit opnemen in het verwerkingsregister.
- *Register van datalekken.* Daarnaast is het verplicht om een register van datalekken bij te houden. Leg alle (vermoedens van) datalekken vast, schrijf op wat u gedaan hebt om het datalek op te lossen en geef aan of en wanneer u het gemeld hebt bij de Autoriteit Persoonsgegevens. Met dit register toont u aan dat u het voorkomen en oplossen van datalekken serieus neemt.
- *Data Protection Impact Assessment (DPIA).* Een Data Protection Impact Assessment betekent dat u (eventueel samen met een externe partij) in kaart brengt waar de risico's zitten als het gaat om gegevensbeveiliging en privacy. Zowel voor de gegevensbescherming als voor uw praktijk zelf levert een DPIA voordelen op.

4. Processen & Facturatie

De vierde en laatste categorie, is een verzameling van een aantal andere zaken die u op orde moet hebben. Kijk kritisch naar de processen in uw organisatie. Zijn die veilig en AVG-proof?

Zorg ervoor dat u uw systemen, processen en de interne organisatie zo hebt ingericht, dat u vanaf 25 mei snel, makkelijk en *op de juiste manier gehoor kunt geven aan verzoeken* van patiënten die betrekking hebben op rechten die zij hebben (zoals beschreven in hoofdstuk 2).

Daarnaast vraagt de AVG van u om de principes ‘privacy by design’ en ‘privacy by default’ als organisatie te omarmen.

- *Privacy by design* houdt in dat u er al bij het ontwerpen, opzetten en ontwikkelen van nieuwe producten en diensten rekening mee houdt dat persoonsgegevens goed worden beschermd.
- *Privacy by default* betekent dat u technische en organisatorische maatregelen neemt om te zorgen dat u alleen noodzakelijke persoonsgegevens verzamelt. Dat wil bijvoorbeeld zeggen; het vakje ‘ja, ik wil de nieuwsbrief ontvangen’ op uw website niet standaard aanvinken.
- Besteed daarnaast aandacht aan *dataminimalisatie*; zo min mogelijk gegevens verzamelen en vermelden op facturen en andere communicatie. Het vermelden van een BSN op een factuur is bijvoorbeeld niet nodig, maar toch gebeurt het nog heel vaak. Als u gegevens niet meer nodig hebt, moet u ze vernietigen.

Factureren & declareren

Bij het proces van factureren en declareren komen heel wat persoonsgegevens kijken. Het is daarom een zeer belangrijk proces om onder de loep te nemen. Gebeurt dit op een veilige en privacy proof manier? Factureren kan voor eerstelijns zorgpraktijken op drie manieren plaatsvinden:

1. *U doet het zelf.* Dan is het belangrijk om de basisvoorzieningen te treffen die gelden vanuit de wet. Verdiep u hier goed in.
2. U werkt met een *administratiekantoor.* U stelt de benodigde patiëntgegevens ter beschikking aan dit kantoor om te verwerken tot facturen, maar blijft zelf de eigenaar van de vorderingen. In dit geval moet u goed onderzoeken of dit administratiekantoor en de partijen waar zij mee samenwerken (de derde schil) AVG-proof werken.
3. U verkoopt facturen aan een *factoringorganisatie.* Omdat een factoringorganisatie door het kopen van de vordering ook eigenaar wordt van de bijbehorende persoonlijke gegevens van uw patiënten, moet u expliciet toestemming van uw patiënten hebben om hun persoonlijke gegevens aan de factoringorganisatie te mogen verkopen. Daarover leest u hieronder meer.

Waar moet u op letten wanneer u een factoringorganisatie inschakelt?

Wanneer u met een factoringmaatschappij in zee gaat, zijn er een paar belangrijke aandachtspunten.

BSN aanleveren is niet atijd toegestaan

Onder de nieuwe wet is het *niet langer toegestaan om een BSN* (burgerservicenummer) aan te leveren aan een partij die tegelijkertijd de eigenaar wordt van de vordering én die de daarbij horende patiëntgegevens gaat verwerken. Bij klassieke factoringorganisaties is dat het geval. Moet u er dan maar voor kiezen om geen BSN aan te leveren? Dat kan, maar het is niet zo verstandig.

De factoringmaatschappij wil - voordat ze een rekening versturen - namelijk checken of iemand verzekerd is. Gebruiken ze daarbij een BSN, dan is het succespercentage 99%. Zonder BSN zakt dat percentage merkbaar, bijvoorbeeld omdat een patiënt is geswitcht van zorgverzekeraar. Alle ‘bounces’ moet de factoringmaatschappij handmatig controleren. Dat kost tijd en geld en dit kunt u op den duur terugzien in de tarieven.

Toestemming vragen verplicht

Wanneer u een vordering verkoopt aan een klassieke factoringpartij die deze ook gaat verwerken, moet u vooraf schriftelijk toestemming vragen aan iedere patiënt of u zijn/haar patiëntgegevens mag delen met de factoringorganisatie.

Dat blijkt uit de expert-analyse van Prof. mr. G.J. Zwenne (hoogleraar Recht en de Informatiemaatschappij aan de Universiteit Leiden en advocaat bij Brinkhof te Amsterdam). Zwenne stelt dat factoringmaatschappijen onder de AVG geen wettelijke grondslag hebben om gezondheidsgegevens van patiënten te mogen verwerken. De Wet marktordening gezondheidszorg (Wmg) biedt volgens Zwenne ook geen soelaas.

Het vragen van toestemming aan iedere patiënt, vergt flink wat administratieve inspanningen.

Wat wordt in de AVG bedoeld met...

Verwerkingsverantwoordelijke: dit bent u als zorgaanbieder. U bent verantwoordelijk voor de wijze waarop gegevens van uw patiënten worden verwerkt.

Verwerker: dit zijn bijvoorbeeld uw administratiekantoor en softwareleverancier. Zij verwerken gegevens van uw patiënten, waarvoor u verantwoordelijkheid hebt.

Betrokkene: dit is uw patiënt, degene wiens persoonsgegevens worden verwerkt.

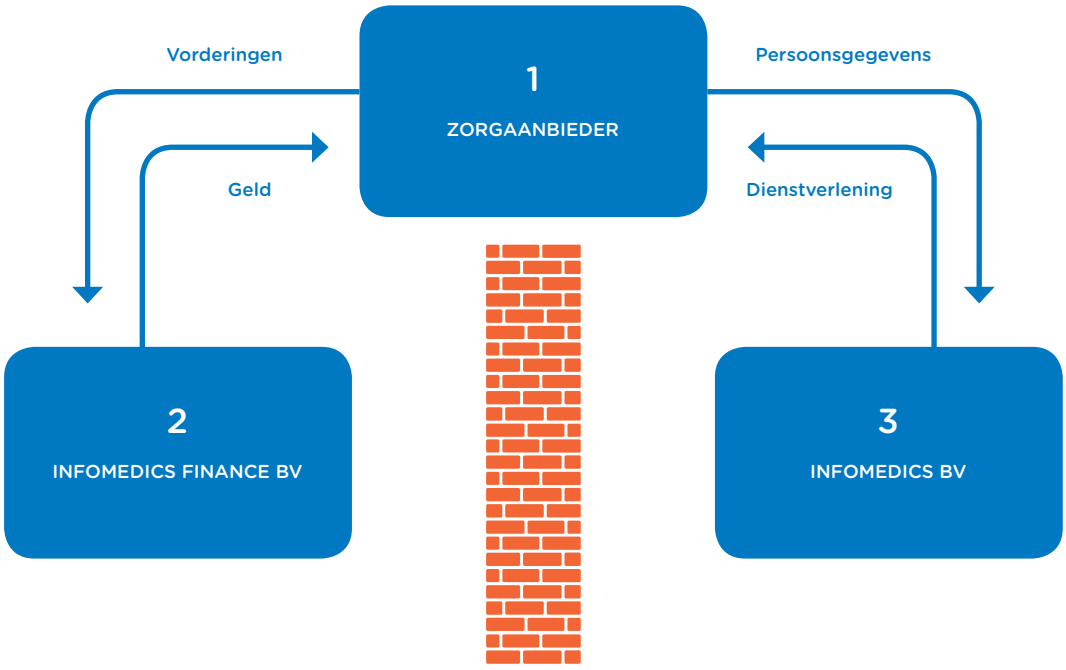
Verwerkersovereenkomst: de overeenkomst tussen zorgaanbieder en verwerker, waarin wordt vastgelegd hoe de veilige verwerking van persoonsgegevens wordt geborgd.

Infomedics werkt als een administratiekantoor

Om te voorkomen dat u toestemming aan uw patiënten moet vragen én om te kunnen blijven werken met het BSN heeft Infomedics er bewust voor gekozen om te werken in *een zogenaamde driepartijenstructuur.*

- *Partij 1.* De eerste partij is de zorgaanbieder, die verkoopt de vordering aan partij 2.
- *Partij 2.* De tweede partij is Infomedics Finance B.V. Deze wordt eigenaar van de vorderingen, maar is niet bevoegd noch in staat om persoonsgegevens van patiënten in te zien of te verwerken. Deze partij staat volkomen los van partij 3, wordt door een onafhankelijke bestuurder beheerd en heeft geen toegang tot de persoonsgegevens die bij de betreffende vorderingen horen. Het enige doel van deze partij is het voorfinancieren van de door zorgaanbieders aangeleverde declaraties.
- *Partij 3.* De derde partij is Infomedics BV. Deze treedt op als administratiekantoor en zet de benodigde persoonsgegevens om in facturen. Infomedics werkt als verwerker onder de verantwoordelijkheid van de zorgaanbieder. De zorgaanbieder ziet er op toe dat Infomedics BV de persoonsgegevens van zijn patiënten met de grootst mogelijke zorgvuldigheid verwerkt. De afspraken hierover hebben de zorgaanbieder en Infomedics BV vastgelegd in een verwerkersovereenkomst.

Omdat de verwerking van de informatie is gescheiden van het eigendom, mag Infomedics het BSN verwerken en hoeft u als zorgaanbieder *geen toestemming aan uw patiënten te vragen* om hun persoons- en behandelgegevens met Infomedics te mogen delen.



CHECKLIST

1. Bewustzijn & Gedrag

- ☐ Staat het bespreken van dataveiligheid & privacy hoog op de agenda?
- ☐ Is de bewustwording van het hele team op orde?
- ☐ Worden wachtwoorden regelmatig veranderd & veilig bewaard?
- ☐ Zijn verlaten werkstations altijd vergrendeld?
- ☐ Wordt de clean desk policy goed nageleefd?
- ☐ Worden (vermoedelijke) datalekken gemeld bij de Autoriteit Persoonsgegevens?

2. Hardware & Software

- ☐ Zijn uw computers en beveiliging gecheckt en geüpgraded door een ICT-expert?
- ☐ Is thuis- en on the road werken goed beveiligd?
- ☐ Zijn computers met patiëntendata onbereikbaar voor derden?
- ☐ Is de praktijksoftware en andere software die u gebruikt AVG-proof?

3. AVG: Eisen & Documentatie

- ☐ Hebt u een privacyverklaring op de website/in de wachtkamer?
- ☐ Hebt u een verwerkersovereenkomst afgesloten met partijen die voor u gegevens verwerken?
- ☐ Hebt u een intern privacybeleid opgesteld?
- ☐ Hebt u een verwerkingsregister?
- ☐ Hebt u een register van (vermoedelijke) datalekken?
- ☐ Hebt u (indien nodig) een DPIA (data protection impact assessment) uitgevoerd?

4. Processen & Facturatie

- ☐ Kunnen patiënten eenvoudig hun rechten uitoefenen?
- ☐ Let u actief op dataminimalisatie?
- ☐ Hebt u het proces van declareren & factureren AVG-proof ingericht?

Privacy & dataveiligheid

Het zit in ons DNA

Privacy en dataveiligheid worden voor de patiënten en eerstelijns zorginstellingen alsmaar belangrijker. Een goede ontwikkeling, die wij van harte toejuichen. Aandacht voor privacy en dataveiligheid zit namelijk in het DNA van Infomedics.

ISO27001

Infomedics is al sinds 2015 ISO27001-gecertificeerd. Dit is de strengste privacycertificering en houdt in dat we maar liefst 114 concrete normen naleven om zo veilig mogelijk te werken. Daarop worden we elk jaar gecontroleerd door onafhankelijke auditors van Lloyd's Register. Daarnaast zijn we speciaal voor de zorg NEN7510-gecertificeerd.

Wij stimuleren actief een privacy proof cultuur onder onze medewerkers. Zo organiseren we twee keer per jaar een bewustwordingssessie omtrent privacy, die alle medewerkers moeten bijwonen. Daarnaast gebruiken we de app Knowingo, een kennistest waarin collega's het tegen elkaar opnemen. Privacy en de bescherming van persoonsgegevens vormen een belangrijk onderdeel van deze test.

Dat we onze datazorgplicht serieus nemen, is ook de reden dat we deze whitepaper schrijven en onze kennis hierover met u delen. De wetgeving is de afgelopen jaren immers zo complex geworden, dat het voor eerstelijns zorgpraktijken een flinke kluif is geworden om alles op een goede manier te regelen.

Wilt u meer weten over privacy proof declareren & factureren? We denken graag met u mee! Neem voor vragen contact op met onze collega's van de servicedesk via **servicedesk@infomedics.nl** of bel ons op **088 6555 987.**

Infomedics B.V.
Postbus 60108
1320 AC Almere
P.J. Oudweg 4
1314 CH Almere
Tel. 088 6555 987

www.infomedics.nl

infomedics