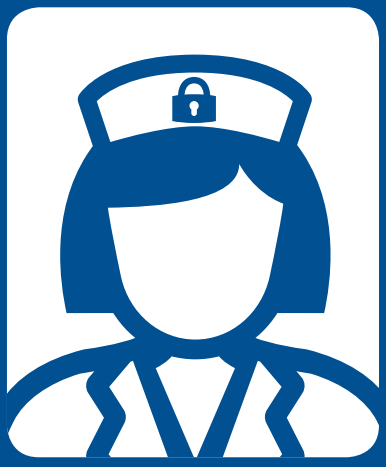
#ditisprivé



Whitepaper

# Een nieuwe privacywet

## (en wat dat betekent voor de zorgwereld)

Cijfers, valkuilen en tips

#ditisprivé

# Een nieuwe privacywet

## (en wat dat betekent voor de zorgwereld)

Hoe gaan we binnen de Nederlandse zorgwereld om met privacygevoelige informatie? En waar moeten we aan voldoen als in mei 2018 de nieuwe Europese privacywet van kracht wordt? **Je leest het in deze whitepaper.**

Cijfers, valkuilen en tips

#ditisprivé

# De cijfers

## 2 petabyte per jaar

**Dat is de geschatte dataproductie door Nederlandse ziekenhuizen. Als je die data op dvd's zou bewaren, heb je 500.000 schijfjes nodig. En die denkbeeldige stapel zal nog flink groeien. Het toenemend gebruik van sensoren, apps en elektronische dossiers gaat binnen de zorg namelijk nog veel meer data opleveren.**

Bron: 'De zorgzame informatiesamenleving', visiedocument van ECP

## 165.000 apps in categorie Zorg & Gezondheid

**En daarvan zijn er volgens ECP (Platform voor Informatiesamenleving) enkele honderden afkomstig van Nederlandse artsen, ziekenhuizen, zorgverzekeraars en farmaceutische bedrijven.**

Bron: 'De zorgzame informatiesamenleving', visiedocument van ECP

## 50%

## Bijna helft van ziekenhuizen heeft een patiëntportaal

Dat was halverwege 2017. Een jaar eerder waren dat er nog maar 22. In een jaar tijd is het aantal ziekenhuizen met een patiëntportaal bijna verdubbeld. Dat betekent dat steeds meer patiënten online inzage hebben in hun medische dossier en diagnostische uitslagen.

Bron: Digitale Zorg Gids, Patiëntenfederatie Nederland

#ditisprivé

# De overheid moedigt digitalisering van de zorg aan

## Zo wil het ministerie van Volksgezondheid, Welzijn en Sport (VWS) dat in 2019...

... 80% van de chronisch zieken (en 40% van de overige Nederlanders) direct toegang heeft tot bepaalde medische gegevens, waaronder medicatie-informatie, vitale functies en testuitslagen – en dat ze die gegevens desgewenst kunnen gebruiken in mobiele apps of internetapplicaties.

... driekwart van de chronische zieken (bijvoorbeeld mensen met diabetes of COPD) en kwetsbare ouderen zelfstandig metingen kunnen uitvoeren. Als ze dat tenminste willen en daar ook toe in staat zijn. En die zelfmeting zal dan in de meeste gevallen gecombineerd worden met gegevensmonitoring op afstand door de zorgverlener.

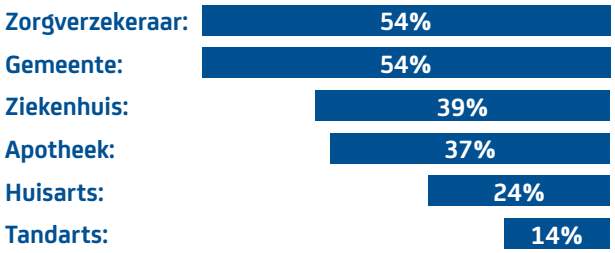
... iedereen die thuis zorg en ondersteuning ontvangt, de mogelijkheid krijgt om via een beeldscherm met een zorgverlener te communiceren. En dan niet op bepaalde uren, maar 24/7. Die optie is op vrijwillige basis. Naast beeldschermzorg zal er ook domotica (huisautomatisering) worden ingezet.

Bron: www.rijksoverheid.nl

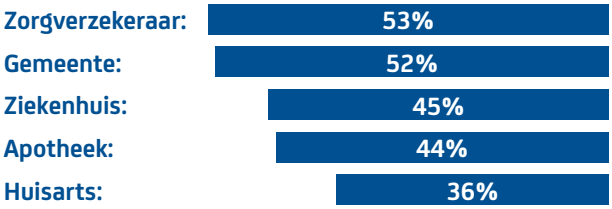
# Zorgen over de veiligheid

Die zijn er ook. Digitale monitoring van patiënten en het elektronisch delen van medische gegevens levert namelijk ook risico op. Niet iedereen is ervan overtuigd dat er zorgvuldig met die privacygevoelige informatie wordt omgegaan.

*Percentage Nederlanders dat zich zorgen maakt over de veiligheid van hun medische gegevens:*




*Percentage dat onvoldoende weet over de veiligheid van het medische dossier:*




Aan de hand van deze cijfers trekt de Patiëntenfederatie Nederland de volgende conclusie: “Hoe minder mensen weten over de veiligheid, hoe meer zorgen ze zich hierover maken”.

Bron: ‘Rapport meldactie ‘Privacy’’, van de Patiëntenfederatie Nederland

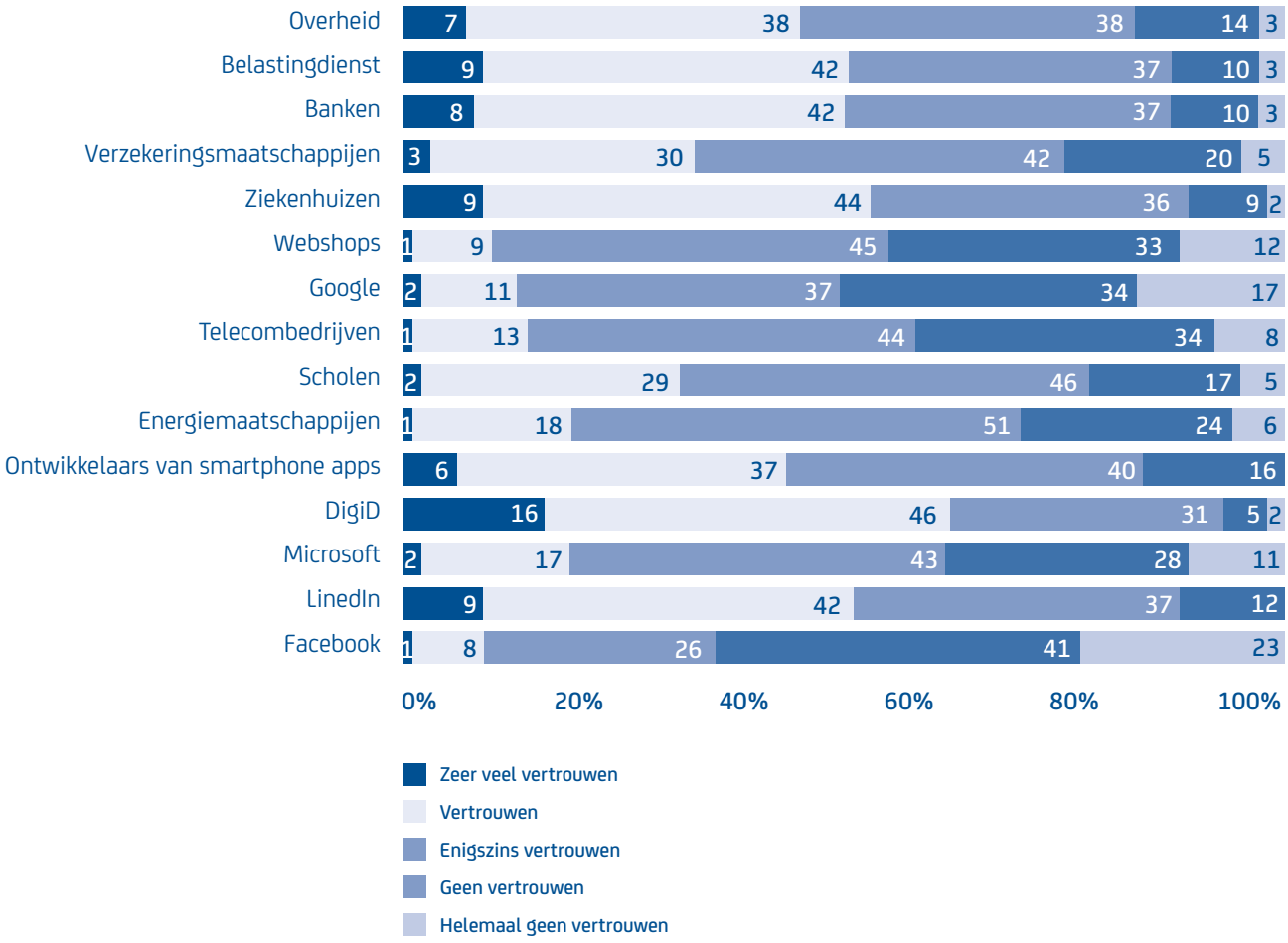
#ditisprivé

# 53% heeft er vertrouwen in dat ziekenhuizen veilig met persoonlijke gegevens omgaan

Dat blijkt uit een ander onderzoek, uitgevoerd door Capgemini. Ziekenhuizen blijken daarin beter te scoren dan de overheid (45%). DigiD was met 62% de koploper. En de ontwikkelaars van smartphone-apps bungelden met 6% onderaan die lijst.

Bron: 'Trends in Veiligheid 2017', van Gapgemini

**Hoeveel vertrouwen heeft u erin dat de volgende instanties veilig met uw gegevens omgaan?**



Valkuilen

# Big data, toenemende complexiteit en pittige sancties

**Elektronische uitwisseling van patiëntgegevens, big data-onderzoeken en super-computers die helpen bij het stellen van diagnoses. De digitalisering van de zorg zit in een stroomversnelling. Dat brengt ook uitdagingen met zich mee. Want hoe houd je grip op die enorme informatiestroom? En hoe scherm je privacygevoelige informatie af?**

**Gezondheidsgegevens zijn gevoelig** en in de Wet bescherming persoonsgegevens (Wbp) worden die dan ook als bijzondere persoonsgegevens aangemerkt. Dat betekent dat je die gezondheidsgegevens alleen onder bepaalde voorwaarden mag gebruiken. En let op: het gaat daarbij om alle gegevens die betrekking hebben op iemands lichamelijke of geestelijke gezondheid, dus niet alleen om de medische gegevens die artsen vaststellen en vastleggen.

**Big data** maken het mogelijk om razendsnel verbanden te vinden, maar dus ook verbanden die privacygevoelig zijn... In de VS merkte de gouverneur van Massachusetts, William Weld, in 1997 al wat er kan gebeuren als mensen verschillende informatiebronnen met elkaar vergelijken. Een overheidsorganisatie in zijn staat had een zorgverzekering voor ambtenaren ingekocht. De geanonimiseerde declaratiegegevens van de verzekerden werden vervolgens beschikbaar gesteld voor onderzoek. Namen, adressen en sociale verzekeringsnummers waren uit die database verwijderd. Wel stonden de geboortedata en postcodegebieden er nog in. Weld verzekerde dat de privacy van alle betrokken gegarandeerd was. Dat had hij beter niet kunnen doen, want MIT-student Latanya Sweeney ging de uitdaging aan: met behulp van de stemlijst van Cambridge, Massachusetts (de stad met 54.000 inwoners waar de gouverneur woonde) wist ze hem al snel in de geanonimiseerde gegevens te vinden. De gouverneur was not amused toen hij niet lang daarna een brief van Sweeney ontving met daarin zijn medische gegevens, inclusief diagnosen en voorgeschreven medicatie. En dat was al twintig jaar geleden! Tegenwoordig kunnen super- computers in no-time een groot aantal databases doorspitten en daar hun kunstmatige intelligentie op loslaten. In dit Big Data-tijdperk is het dus nog veel lastiger om gegevens te anonimiseren.

Bronnen: 'Big data in de zorg', van de Wetenschappelijke Raad voor Regeringsbeleid (WRR) en Forbes.com

**Het medisch beroepsgeheim** geldt uiteraard ook in de digitale wereld. In Nederland zijn er partijen die wijzen op het spanningsveld tussen datadeling en het medisch beroepsgeheim. Zo is er de Stichting KDVP die in 2007 werd opgericht en die er sindsdien op blijft hameren dat ook het geanonimiseerd delen van medische informatie privacyrisico's met zich meebrengt.

**Van wie zijn de gegevens?** Wanneer is het belang van onderzoek of zorgtoepassing groter dan de privacy van de patiënt? En wie mogen de data gebruiken? Dat zijn enkele vragen die ECP, Platform voor de Informatiesamenleving, in een visiedocument stelt. Maar die vragen zijn lang niet altijd op een eenduidige manier te beantwoorden. Veel hangt af van de situatie, de manier waarop de gegevens zijn verkregen en of patiënten al dan niet toestemming hebben gegeven voor het delen van die gegevens. Gezondheidswinst zou leidend moeten zijn, vindt ECP, met daarbij de kanttekening dat het privacybelang wel altijd afgewogen moet worden terwijl het lang niet altijd duidelijk is wie daar over gaat. Complexe materie dus, vooral als er meerdere partijen bij betrokken zijn.

Bron: 'De zorgzame informatiesamenleving', visiedocument van ECP

**De privacyregels worden regelmatig aangepast** en je zult je echt goed in dat onderwerp moeten verdiepen om precies te weten wat er al dan niet is toegestaan. Niet zo gek dat steeds meer organisaties besluiten om een functionaris voor de gegevensverwerking (FG) aan te stellen. In mei 2018, als de Algemene verordening gegevensbescherming (AVG) ingaat, zal dit voor bepaalde organisaties zelfs verplicht worden. Maar dus niet voor elke organisatie. Dat is een aandachtspunt, vooral omdat er straks fikse boetes zullen worden uitgedeeld aan partijen die zich niet aan de nieuwe privacywet houden. Om precies te zijn: de Autoriteit Persoonsgegevens (AP) kan organisaties sancties opleggen van maximaal 20 miljoen euro of 4% van hun wereldwijde omzet. Het overschrijden van de nieuwe privacywet kan straks dus flink pijn doen.

#ditisprivé

# 10 TIPS

## 25 mei 2018: vanaf die dag geldt dezelfde privacywetgeving in de hele EU. In Nederland gaat het om de Algemene verordening gegevensbescherming (AVG). Maar wat moet je allemaal doen om je op die nieuwe privacywet voor te bereiden? Het tien-stappen-plan van de Autoriteit Persoonsgegevens:

1 **Bewustwording** De AVG kan invloed hebben op de huidige werkprocessen en de manier waarop goederen en diensten tot stand komen. Dat betekent dat de betrokken binnen een organisatie goed op de hoogte moeten zijn van de nieuwe privacyregels. Nadat zij een inschatting hebben gemaakt van de impact van de AVG, moeten de benodigde aanpassingen natuurlijk ook nog worden doorgevoerd. Dat kan aardig wat tijd en menskracht kosten. Begin daar dus op tijd mee!

2 **Houd er rekening mee dat betrokkenen straks meer en verbeterde privacyrechten krijgen.** Naast de bestaande rechten (bijvoorbeeld het recht op inzage en het recht op correctie en verwijdering), komen er met de komst van de AVG ook nieuwe rechten, zoals het recht op dataportabiliteit. Iedereen van wie u persoonsgegevens verwerkt moet de mogelijkheid hebben om die gegevens makkelijk te krijgen en desgewenst aan een andere organisatie door te geven. Als mensen die mogelijkheid niet krijgen, kunnen ze bij de AP een klacht indienen.

3 **Breng alle gegevensverwerkingen goed in kaart.** Welke persoonsgegevens verwerk je? Met welk doel? Waar komen die gegevens vandaan? En met wie deel je ze? Op die vragen moet je straks ondubbelzinnig antwoord kunnen geven. Onder de AVG heb je namelijk een verantwoordingsplicht.

4 **Schat alvast in of je straks een privacy impact assessment (PIA) moet uitvoeren.** Dat wordt onder de AVG verplicht als de beoogde gegevensverwerking een hoog privacyrisico met zich meebrengt. Blijkt uit de PIA inderdaad dat er een hoog risico is en is het lastig om maatregelen te nemen om dat risico te beperken? Neem dan contact op met AP. Die beoordeelt dan of de voorgenomen verwerking al dan niet in strijd is met de AVG.

5 **Wordt vertrouwd met de begrippen Privacy by design & Privacy by default.** Onder de AVG worden dat verplichte uitgangspunten. Bij Privacy by design zorg je er bij het ontwerpen van producten en diensten al voor dat persoonsgegevens op een goede manier worden beschermd. Privacy by default houdt in dat je alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat je wilt bereiken. Een app mag bijvoorbeeld niet de locatie van gebruikers registreren als dat niet nodig is.

6 **Check of het straks nodig is om een functionaris voor de gegevensverwerking (FG) aan te stellen.** Onder de AVG wordt dat voor bepaalde organisaties verplicht. Geldt dat ook voor jouw organisatie? Begin dan meteen met de werving. Vrijwillig een FG aanstellen mag uiteraard ook.


#ditisprivé

7 **Documenteer alle datalekken zorgvuldig.** Onder de AVG blijft de meldplicht datalekken grotendeels hetzelfde als nu. Wel komen er strengere eisen voor het zelf registreren van datalekken.

8 **Zorg bij het uitbesteden van gegevensverwerking dat ook de bewerker voldoet aan de eisen.** Zijn de afspraken in bestaande contracten nog actueel en welke maatregelen neemt de bewerker om straks aan de verplichtingen van de AVG te voldoen?

NB: een bewerkersovereenkomst is een handige manier om afspraken met bewerkers vast te leggen. De Nederlandse Vereniging van Ziekenhuizen heeft dan ook een model-bewerkersovereenkomst ontwikkeld (alleen voor leden).

9 **Weet wie straks de leidende privacy-toezichthouder wordt.** Vestigingen in meerdere EU-lidstaten? Of heeft je gegevensverwerkingen in meerdere lidstaten impact? Dan krijg je straks, onder de AVG, nog maar met één toezichthouder te maken.

10 **Evalueer de manier waarop je toestemming vraagt voor het verwerken van gegevens.** De AVG stelt strengere eisen aan die toestemming. Nieuw daarbij is dat je moet kunnen aantonen dat je van mensen geldige toestemming hebt gekregen om hun persoonsgegevens te verwerken. Ook nieuw: het moet voor mensen net zo makkelijk zijn om hun toestemming in te trekken als om die te geven.

Gedetailleerde informatie over de bovenstaande stappen is te vinden op de website van Autoriteit Persoonsgegevens.

#ditisprivé

checklist

# Het medisch beroepsgeheim...

## ✓ Wanneer mogen/moeten zorgverleners medische informatie delen?

**Voor iedereen die met medische gegevens te maken krijgt, geldt een geheimhoudingsplicht. Voor artsen, tandartsen, GZ-psychologen, psychotherapeuten, fysiotherapeuten, verloskundigen en verpleegkundigen gaat het nog een stap verder: zij zijn gebonden aan een wettelijk vastgelegd medisch beroepsgeheim.**

### Zorgverleners mogen medische informatie wel delen met...

...degenen die rechtstreeks bij de behandeling van een patiënt betrokken zijn. Dat kunnen andere zorgverleners zijn, maar bijvoorbeeld ook secretaresses of financieel medewerkers die de gegevens nodig hebben om hun werk te kunnen doen. Als de patiënt hier bezwaar tegen maakt, mag de zorgverlener de medische gegevens niet verstrekken. Landelijke uitwisseling via een elektronisch patiëntendossier mag alleen als de patiënt daar vooraf toestemming heeft gegeven. Soms geldt dat ook voor regionale uitwisseling.

...wettelijke vertegenwoordigers. Maar alleen als dat nodig is om hun toestemming te vragen voor de behandeling van een kind onder de 16 jaar of een wilsonbekwame patiënt.

...personen of teams die wetenschappelijk onderzoek doen. Zij mogen alleen medische gegevens krijgen van patiënten die daar toestemming voor hebben gegeven. In sommige gevallen mag dat ook zonder toestemming, maar dan moet de zorgverlener wel kunnen uitleggen waarom het redelijkerwijs niet mogelijk of gewenst was om die toestemming te vragen. Los van de toestemming, moet de zorgverlener er altijd voor zorgen dat de privacy van zijn patiënten gewaarborgd blijft.

### Enkele redenen om het medisch beroepsgeheim te doorbreken:

**Toestemming van de patiënt:** een zorgverlener mag medische gegevens van een patiënt aan anderen doorgeven als de patiënt hem daar toestemming voor heeft gegeven. Daarbij geldt wel een informatieplicht: de patiënt moet dus weten waarom de zorgverlener zijn medische gegevens aan anderen wil verstrekken.

**Wettelijk voorschriften:** soms schrijft de wet voor dat een zorgverlener medische gegevens moet delen. Zo is er de Wet publieke gezondheid waarin staat dat een zorgverlener bepaalde besmettelijke ziekten direct bij de GGD moeten melden.

**Conflict van plichten:** als het vasthouden aan het medisch beroepsgeheim ernstig nadeel of zelfs gevaar oplevert voor de patiënt of iemand anders, mag de zorgverlener het medisch beroepsgeheim doorbreken. Het moet echt een noodsituatie zijn. Kindermishandeling bijvoorbeeld.

Bron: Autoriteit Persoonsgegevens

**Meer weten?**
Kijk op medireva.nl/ditisprive en schrijf je in voor de nieuwsbrief.

MediReva

#ditisprivé

**Meer weten?**
medireva.nl/ditisprive

MediReva