nvm mondhygiënisten

Privacybeleid

“OpJeLip”

Datum: 25-5-18

Versie: 1

nvm mondhygiënisten

Inhoudsopgave

nvm mondhygiënisten

1. Inleiding

De AVG treedt met ingang van 25 mei 2018 in werking. Vanaf dat moment gelden er voor alle Europese landen dezelfde regels rondom de verwerking van persoonsgegevens. Daarnaast zijn deze regels aangescherpt. Een voorbeeld: waar voorheen veronderstelde toestemming door niet reageren ook als toestemming voldoende was, is dit nu veranderd in uitdrukkelijke toestemming door een actieve handeling (bijvoorbeeld handtekening na aanvinken).

Handleiding privacybeleid na invoering AVG toolkit

Dit privacybeleid is een handleiding voor praktijken hoe met verscherpte regels rondom bescherming van persoonsgegevens om te gaan. Onder de AVG moet verwerking van persoonsgegevens een grondslag hebben. Deze grondlagen staan opgesomd in de toelichting van de toolkit. Als verwerking is toegestaan, moet rechtmatig, behoorlijk en transparant worden gehandeld, moet er sprake zijn van beveiliging en mogen gegevens niet langer worden bewaard dan nodig. Ook moet bewust worden nagedacht over de noodzaak van verwerking. “Is het voor deze dienst echt nodig om een geboortedatum op te vragen?”

In dit privacybeleid is in hoofdstukken gedocumenteerd welke factoren van belang zijn voor een goed privacybeleid. Dit correspondeert met het stappenplan voor de invoering van de AVG. Elke stap uit het stappenplan is in een hoofdstuk opgenomen.

Hebt u vragen bij het implementeren en uitvoeren van dit privacybeleid? Hiervoor kunt u contact opnemen met Marjolein Stigter van NVM-mondhygiënisten. U kunt uw vraag via de mail stellen: AVG@mondhygienisten.nl

Algemene uitganspunten

De praktijk voert een privacybeleid uit, dat is gebaseerd op een aantal uitgangspunten. Hieronder staan deze kort genoemd.

- Voor verwerking van (bijzondere) persoonsgegevens buiten die gegevens die noodzakelijk zijn voor de behandelovereenkomst met de patiënt, is uitdrukkelijke toestemming vereist. Voorbeeld: verzending nieuwsbrief.
- Persoonsgegevens worden alleen verwerkt voor het doel waarvoor zij zijn verstrekt.
- Persoonsgegevens worden niet aan derden verstrekt, tenzij dit nodig is voor de uitvoering van de doeleinden waarvoor ze zijn verstrekt.
- Persoonsgegevens die nodig zijn voor de doeleinden van de praktijkvoering worden verwerkt en geen andere die hiervoor niet noodzakelijk zijn.
- De praktijk heeft de juiste technische en organisatorische maatregelen genomen ter bescherming van de verwerkte persoonsgegevens.

- De praktijk informeert personen van wie persoonsgegevens worden gebruikt over de rechten die zij in dit kader hebben in een privacyverklaring.

Het privacybeleid wordt periodiek geëvalueerd en, indien nodig, aangepast.

Voor vragen over het privacybeleid of andere vragen over de bescherming van persoonsgegevens binnen de praktijkvoering kan contact worden opgenomen met:

Praktijknaam	OpJeLip
Contactpersoon	Birgitta Ruijs
Adres	Dalweg 172
Postcode	6865CX
Plaats	Doorwerth
E-mailadres	ojl@opjelip.nl
Telefoonnummer	06-14822033

Na invoering van het privacybeleid is het van belang dat de met privacy belaste medewerker (kunt u ook zelf zijn) periodiek, het beleid controleert en evalueert. Hierbij kan het privacybeleid eventueel ook worden aangepast.

2. Persoonsgegevens en verwerkingsregister

Ter uitvoering van de behandelovereenkomsten met patiënten worden persoonsgegevens van patiënten verwerkt. Dit zijn “gewone persoonsgegevens” zoals NAW- gegevens, waarbij gegevens herleidbaar zijn tot een persoon, maar ook bijzondere persoonsgegevens zijn noodzakelijk ter uitvoering van de behandelovereenkomst. Bijzondere persoonsgegevens zijn iets meer gevoelige gegevens omtrent iemands gezondheid, medische geschiedenis, medicatiegebruik. Deze persoonsgegevens zijn vaak meer gevoelig dan bijvoorbeeld NAW-gegevens. Hieronder staan de persoonsgegevens die in de praktijk worden verwerkt gecategoriseerd in beeld.

Persoonsgegevens	**Bijzondere persoonsgegevens**
NAW -gegevens	Medische gegevens medicatiegebruik
geboortedatum	Medische gegevens gezondheid
Telefoonnummer	BSN nummer
E-mailadres	
Burgerlijke staat	
Geslacht	
Verzekeringsgegevens	

Voor verwerking van persoonsgegevens is op grond van de AVG een grondslag (doel) vereist. Deze staan opgesomd in de toelichting van de toolkit. Is er geen grondslag, dan is de verwerking niet toegestaan. De praktijk verwerkt persoonsgegevens onder de volgende

grondslagen. De rood gearceerde stukken tekst moeten op het intakeformulier worden overgenomen, zodat de vereiste toestemming ook door de patiënt wordt gegeven.

- Verwerking van (bijzondere) persoonsgegevens is noodzakelijk ter uitvoering van een behandelovereenkomst met de patiënt. Bij het sluiten van de behandel-overeenkomst/aangaan behandelrelatie wordt de patiënt op het intakeformulier hiervoor om uitdrukkelijke toestemming door middel van handtekening verzocht. Hieronder vallen de volgende verwerkingen.

    - Verzenden van afspraak herinneren middels sms- of e-mailbericht
    - Het factureren van de behandelingen aan de patiënt.
    - Bijzondere persoonsgegevens zoals medische gegevens over gezondheid en medicatiegebruik zijn noodzakelijk voor een goede medische anamnese en zorgvuldige medische behandeling van de patiënt.
    - Bijzondere persoonsgegevens zoals BSN-nummer en nummer identificatiedocument zijn noodzakelijk ter uitvoering van een wettelijke verplichting van de zorgaanbieder de patiënt voldoende te identificeren.

- Verwerking van (bijzondere) persoonsgegevens is daarnaast tevens nodig voor andere doelen dan specifiek de uitvoering behandelovereenkomst.

    - Verzenden van nieuwsbrieven aan patiënten. Patiënten wordt hiervoor op het aanmeldformulier uitdrukkelijk om toestemming gevraagd.
    - In geval de praktijk deelneemt aan onderzoeken binnen het project Peilstations, worden gegevens verstrekt aan de beroepsvereniging NVM-mondhygiënisten.
    - Op grond van de Wkkgz dient elke praktijk een Veilig Incident Melden systeem te hebben, waarbij incidenten door medewerkers worden gemeld, zodat kwaliteit van zorg kan worden verbeterd en gewaarborgd. Dit vindt op anonieme basis plaats, tenzij er zich risico's voor de patiënt hebben voorgedaan. In dit geval wordt de patiënt hierover ingelicht.

Bij het sluiten van de behandelovereenkomst/aangaan behandelrelatie wordt de patiënt op het intakeformulier verzocht om uitdrukkelijke toestemming te geven voor het verwerken van persoonsgegevens voor doelen die *anders* zijn dan de specifieke uitvoering van de behandelovereenkomst, zie de opsomming hierboven.

Let op: hierbij moet specifiek per verwerking en per doel om uitdrukkelijke toestemming worden gevraagd. Voorbeeld: toestemming voor verzending van een nieuwsbrief is niet voldoende. Hierbij moet worden aangegeven via welk kanaal, hoe vaak deze wordt

verzonden. Indien er verschillende nieuwsbrieven worden verzonden, dient dan ook per nieuwsbrief uitdrukkelijke (vink) toestemming te worden gegeven. In de nieuwsbrief zelf moet een mogelijkheid zijn opgenomen waar de ontvangen zich kan afmelden.

Wanneer is de praktijk wettelijk verplicht om persoonsgegevens te delen?

Op grond van onder meer de Wkkgz is IGJ (inspectie) onder andere belast met toezicht en handhaving op de zorg in het kader van calamiteiten en geweld bij de zorgverlening of ernstig disfunctioneren van een medewerker. IGJ is in die situatie wettelijk gerechtigd dossiers op te vragen en in te zien. De praktijk is gehouden hieraan medewerking te verlenen.

De NZa is toezichthouder op de markt. Uit dien hoofde heeft de NZa recht op inzage in gegevens waaronder medische dossiers, waaraan de praktijk wettelijk gezien medewerking dient te verlenen.

Alle verwerkingen van de hierboven genoemde persoonsgegevens zijn geregistreerd in een verwerkingsregister persoonsgegevens. Dit verwerkingsregister vindt u in de NVM AVG toolkit. Het verwerkingsregister moet periodiek gecontroleerd worden op actualiteit en juistheid door de praktijkmedewerker die met uitvoering van het privacybeleid is belast.

De AP kan bij een controle verzoeken om inzage in het verwerkingsregister persoonsgegevens.

nvm mondhygiënisten

3. Technische en organisatorische maatregelen

Op grond van de AVG moeten bedrijven, instanties en zorgaanbieders maatregelen nemen om onrechtmatige verwerking van persoonsgegevens en datalekken tegen te gaan. Hieronder staan een aantal maatregelen die genomen moet worden. Daarnaast kan de NEN 7510 inzicht bieden in wat de praktijk nog meer kan doen in het kader van informatiebeveiliging (meer info: www.werkenmetnen7510.nl). De praktijk heeft de volgende maatregelen genomen.

□ De mevrouw B. Ruijs is binnen de praktijk aanspreekpunt voor de informatiebeveiliging en actualiseert jaarlijks de maatregelen en afspraken zoals hieronder benoemd.

□ De praktijk werkt met patiënten softwaresysteem: Exquise

- Met de leverancier van dit softwaresysteem is een bewerkersovereenkomst gesloten. Daarnaast zijn afspraken gemaakt over veilig aansluiten of installeren van applicaties/programma's.
- De software is alleen toegankelijk voor daartoe bevoegd en geschoold personeel.
- De software/systemen zijn beveiligd met inlogcodering en autorisaties. Privacy van persoonsgegevens is gewaarborgd.
- De systemen waarmee wordt gewerkt, zijn doorlopend beschikbaar en actueel.
- Patiëntendossiers zijn altijd zo actueel mogelijk.
- Bij mobiel inloggen, dan wel werken vanuit huis wordt veilig gewerkt.
- Binnen het patiëntensysteem zijn alle patiëntgegevens gekoppeld aan het BSN.
- Er is een goede afweer tegen virussen, spam en andere gevaren van buitenaf.
- Niet actuele patiëntgegevens worden mimimaal 15 jaar bewaard, tenzij op verzoek van patiënt vernietiging heeft plaatsgevonden.

□ Praktijkmedewerkers hanteren een clean desk en clean screen policy. Systemen worden uitgezet bij verlaten van de werkplek. Systemen worden versleuteld en zijn zo nodig geautoriseerd.

□ Uitwisseling van informatie, communicatie tussen collega's vindt altijd veilig plaats. E-mailverkeer tussen collega's en tussen de praktijk en patiënten is beveiligd.

□ De praktijk werkt volgens het protocol meldplicht datalekken.

□ Waarborgen van privacy van de persoonsgegevens binnen de praktijk is een regelmatig terugkerend agendapunt.

nvm mondhygiënisten

4. Verwerkersovereenkomst

In de praktijk wordt samengewerkt met derde partijen ter uitvoering van de behandelovereenkomst met de patiënt. De praktijk is en blijft eindverantwoordelijke voor een goede en veilige omgang met de persoonsgegevens van patiënten. Om dit te kunnen waarborgen is met alle derde partijen een verwerkersovereenkomst gesloten. Een model verwerkersovereenkomst is opgenomen in de AVG toolkit. In dit model zijn gele tekstdelen opgenomen die u moet invullen. De rode tekstdelen zijn bepalingen die in de verwerkersovereenkomst moeten zijn opgenomen.

Samenwerking met derden ter uitvoering van de behandelovereenkomst.

De praktijk heeft meerdere doeleinden. Het belangrijkste doel is uitvoering van de behandelovereenkomst. In dit kader mogen persoonsgegevens op grond van de AVG aan derden worden verstrekt voor zover dit hiervoor nodig is.

Voor de uitoefening van de behandelovereenkomst werkt de praktijk samen met onderstaande partijen. Voor deze samenwerking geldt: deze samenwerking is noodzakelijk voor de uitoefening van de behandelovereenkomst, wat betekent dat het delen van persoonsgegevens is toegestaan.

x softwareleverancier patiëntenadministratie

x websitebouwer

x office softwareleverancier

x factoringmaatschappij

x Vecozo

x computer onderhoud

Persoonsgegevens worden niet verstrekt aan derde partijen gezeteld buiten de EU.

nvm
mondhygiënisten

5. Protocol meldplicht datalekken en register datalekken

De praktijk heeft technische en organisatorische maatregelen genomen om een eventueel verlies of onrechtmatige verwerking van persoonsgegevens te voorkomen. Desondanks kan een datalek zich toch voordoen. Hiervoor heeft NVM-mondhygiënisten een protocol meldplicht datalekken en register datalekken ontwikkeld, waarbij tevens een stappenplan geldt, zodat schade zoveel als mogelijk beperkt kan worden. Op het moment dat een datalek zich voordoet, handelt de praktijk conform het protocol datalekken, welke een onderdeel is van de AVG toolkit. Ieder datalek binnen de praktijk wordt geregistreerd in het datalekkenregister.

Ieder datalek moet worden gemeld aan de AP, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zie protocol datalekken.

In het Protocol meldplicht datalekken wordt uitgelegd wanneer een incident een datalek is en wanneer moet worden gemeld aan de AP en aan de betrokkene. Hiervoor zijn schema's opgenomen.

Het is belangrijk dat medewerkers, maar vooral de met privacybeleid belaste medewerker kennis neemt van het Protocol Meldplicht datalekken. Daarnaast moet deze medewerker ook alle datalekken opnemen in het register datalekken. Informatie hierover staat ook in het Protocol meldplicht datalekken.

nvm mondhygiënisten

6. Privacyverklaring ten behoeve van de patiënten

In een privacyverklaring voor patiënten wordt uitgelegd wat de praktijk allemaal doet om de persoonsgegevens te beschermen en hoe met persoonsgegevens wordt omgegaan. Het hebben van een privacyverklaring is onderdeel van de verantwoordingsplicht die een praktijk heeft conform de AVG. Het is dan ook belangrijk dat de maatregelen die een praktijk heeft genomen om te werken volgens de AVG, in de privacyverklaring worden benoemd.

In een privacyverklaring worden opgenomen welke persoonsgegevens worden gebruikt, voor welk doel, en met welke partijen deze gegevens in het kader van de overeenkomst met de praktijk worden gedeeld, zodat dit voor een patiënt transparant wordt. Ook de rechten van de patiënt ten aanzien van de (bijzondere) persoonsgegevens wordt aan de orde gesteld. Hierbij wordt de patiënt ook ingelicht over de eventuele gevolgen van het niet willen verstrekken van (bijzondere) persoonsgegevens, zoals BSN nummer en medische informatie/geschiedenis.

Hoe invullen?

Het model moet op de geel gearceerde plaatsen worden ingevuld door de praktijk zelf. Doe dit nadat het stappenplan uit het model privacybeleid is doorlopen, zodat ook alle informatie die hierin moet worden opgenomen, al bekend is, zoals welke persoonsgegevens worden gebruikt, welke maatregelen zijn genomen, etc.

Privacyverklaring overhandigen aan patiënt en op website

Deze privacyverklaring moet op de website van de praktijk worden geplaatst, zodat de patiënten en anderen voldoende op de hoogte zijn. Deze privacyverklaring moet aan de patiënt overhandigd worden op het moment dat de patiënt het intakeformulier voor de praktijk ontvangt. Op het intakeformulier moet een apart vinkje komen te staan.
De patiënt moet deze aanvinken, zodat vaststaat dat de patiënt bekend is met de privacyverklaring van de praktijk en dus weet waarvoor zijn persoonsgegevens worden gebruikt en waarom. Op het intakeformulier moet ook een apart vinkje worden gemaakt voor toestemming van de patiënt voor het gebruik van NAW-gegevens en e-mailadressen voor doeleinden die niet direct de behandelovereenkomst betreffen. Indien gegevens voor een ander doeleinden worden gebruikt, dient ook voor verwerking ten behoeve van dit doel om toestemming te worden gevraagd. Denk aan bijvoorbeeld verzending van nieuwsbrieven.

nvm mondhygiënisten

7. Privacy by design en privacy by default

Privacy by design en privacy by default zijn twee uitgangspunten die gelden sinds inwerkingtreding van de AVG. Het zijn geen handelingen die kunnen worden uitgevoerd, maar aandachtspunten die bij elke ontwikkeling van diensten, of wijzigingen van praktijkwijzen moeten worden meegewogen.

Privacy by design betekent letterlijk: gegevensbescherming door ontwerp. Het idee is om al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen. Het houdt in dat er al bij de ontwikkeling van producten en diensten aandacht moet zijn voor privacy.

Dit bereik je door niet meer persoonsgegevens dan strikt noodzakelijk te verwerken. Daarnaast moeten standaardinstellingen zo privacyvriendelijk als mogelijk zijn. Dit heet *privacy by default*. Deze laatste is dus eigenlijk onderdeel van privacy by design.

Binnen de praktijk moet de medewerker die als de taakuitvoering van het privacy beleid heeft al in de ontwerpfase worden betrokken bij ontwikkeling van diensten en producten voor de patiënten. Dit om zoveel mogelijk te voldoen aan privacy by design en privacy by default.

8. Document veelgestelde vragen privacy en patiëntenrechten

Persoonsgegevens kunnen zoals ook in de inleiding aangegeven, worden onderverdeeld in twee categorieën: persoonsgegevens en bijzondere persoonsgegevens. Beide categorieën zijn tot de persoon herleidbaar, maar de categorie bijzondere persoonsgegevens zijn gegevens die meer gevoelige informatie over een persoon weergeven, zoals geloofsovertuiging, maar ook medische gegevens. Patiëntgegevens valt onder de categorie bijzondere persoonsgegevens en worden dan ook extra beschermd.

Om een goede bescherming van de patiëntgegevens te waarborgen, wordt er in de praktijk gebruik gemaakt van een document veelgestelde vragen privacy en patiëntenrechten. Hierin staan de rechten van patiënten opgenomen zoals, hoe om te gaan met verzoeken van patiënten, rechten omtrent medische informatie, dossierplicht, etc.

Het is van belang dat alle praktijkmedewerkers kennis hebben genomen van dit document zodat zij zelf goed geïnformeerd zijn, maar ook de patiënten goed kunnen informeren. Het is raadzaam dit document periodiek te actualiseren, eventueel aan te vullen, en onder de aandacht te brengen van de praktijkmedewerkers.