

Privacybeleid

“Mond Zorg Zaandam”

Datum: 11-09-2018

Versie: 1

Inhoudsopgave

1. Inleiding
2. Persoonsgegevens en verwerkingsregister
3. Technische en organisatorische maatregelen
4. Verwerkersovereenkomst
5. Protocol meldplicht datalekken en register datalekken
6. Privacyverklaring ten behoeve van patiënten
7. Privacy by design, privacy by default, bewustwording
8. Document veelgestelde vragen privacy en patiëntenrechten

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-mondhygiënist. U kunt uw vraag via de mail stellen: AVG@mondhygienisten.nl

Algemene uitgangspunten

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	Mond Zorg Zaandam
Contactpersoon	Susanne Disveld-Happe
Adres	Oostzijde 18
Postcode	1502 BG
Plaats	Zaandam
E-mailadres	mondzorg@hetnet.nl
Telefoonnummer	075-6125835

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	nee
Burgerlijke staat	nee
Geslacht	ja
Verzekeringsgegevens	ja

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 behandelovereenkomst/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-mondhygiënist.
 - 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 ontvanger 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.

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 heer / mevrouw Susanne Disveld-Happe 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 minimaal 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.
- Praktijkmedewerkers hebben kennis van de rechten van de patiënt, werken met het document veelgestelde vragen privacy en patiëntenrechten.

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.

- softwareleverancier patiëntenadministratie Exquise
- websitebouwer Bratpack
- factoringmaatschappij Famed
- Vecozo
- * Bio2dental

Samenwerking met derden voor andere doelen dan uitvoering behandelovereenkomst.

De praktijk werkt ook met derden samen waarbij het doel niet direct gericht is op de uitvoering van de behandelovereenkomst. Dit kan zijn communicatie via nieuwsbrieven. Hiervoor is op grond van de AVG wel apart toestemming nodig van de patiënt.

Persoonsgegevens worden niet verstrekt aan derde partijen gezeteld buiten E