Privacybeleid AVG

Beleid

Directieverklaring

De directie van huisartsenpraktijk de Schoterpoort draagt zorg voor het privacybeleid binnen de organisatie. Zij stelt als doel dat de belangen van derden bij informatiebeveiliging voldoende worden beschermd. Zo zal er voortdurend gekeken worden of het systeem nog voldoet aan de wettelijke eisen en zal de directie ervoor instaan om binnen de mogelijkheden van de praktijk de veiligheid van gegevens zo goed mogelijk te beschermen.

Privacyverklaring

Het privacy beleid wordt zowel intern als extern gecommuniceerd. De privacyverklaring wordt gepubliceerd op onze website.

Beheer van gegevens

De directie heeft de verantwoordelijkheid om het privacy beleid intern te communiceren. Dit gebeurt onder andere door het privacy beleid te verspreiden onder alle medewerkers. Tevens wordt er in één van de bewustwordingssessies aandacht besteed aan het privacy beleid.

Een van de assistentes (op dit moment S. Koopmans) is dataverantwoordelijke van huisartsenpraktijk de Schoterpoort.

D*e bekende risico's voor de praktijk worden door middel van* bijvoorbeeld interne audits en *bewustwordingssessies geanalyseerd. Maatregelen op deze bekende risico's zijn hieronder* beschreven:

Informatieclassificatie

De praktijk classificeert alle gegevens van patiënten, medische informatie, informatie over behandeling en alle informatie over medewerkers als gevoelige informatie.

De praktijk verwerkt de volgende gegevens:

- *Gegevens van medewerkers. Deze zijn opgeslagen in het personeelsdossier.*
- *Patiëntengegevens: NAW gegevens, BSN nummer, geslacht, leeftijd, telefoonnummer, emailadres, medische gegevens.*
- *Informatie wordt verwerkt door behandelaars, assistenten en praktijkondersteuners.*
- *Informatie wordt bij verwijzing uitgewisseld met een volgende behandelaar (bijvoorbeeld een specialist). Iedere specialist is zelf verwerkingsverantwoordelijke. Hij verwerkt de persoonsgegevens ter uitvoering van de behandelovereenkomst die hij zelf is aangegaan met de patiënt.*
- *De informatie wordt uitgewisseld met andere behandelaars die nodig zijn voor de goede behandeling.*
- *Informatie wordt uitgewisseld met verzekeraars of hun vertegenwoordigers (Vecozo).*

De patiënt kan zijn/haar gegevens op verzoek altijd inzien.

Dataveiligheid door medewerkers/personeel

Beleid bewustwording dataveiligheid door medewerkers

In het contract van iedere medewerker zijn bepalingen over geheimhouding van gegevens en de verantwoordelijkheid om veilig met data om te gaan opgenomen.

Deze bepalingen worden regelmatig benoemd naar de medewerkers. Dit wordt onder andere aangehaald in bewustwordingssessies (in ieder geval 3x per jaar, tijdens de huisartsen-assistenten-overleggen). Tevens worden hier ontwikkelingen op het gebied van dataveiligheid (breed) verspreid en besproken.

Toegangsbeveiliging van data

Autorisatiematrix

	Toegang tot:					
Medewerker	***Patiënt gegevens***	***Financiële gegevens***	***Personeels gegevens***	***Website***		
huisarts	*X*	*X*	*X*	*X*		
huisarts in dienst	*X*			*X*		
waarnemend huisarts	*X*					
POH	*X*					
assistente	*X*					
praktijkassistente	*X*	*X*	*X*			

Organisatie van de informatiebeveiliging op de praktijk.

Huisartsenpraktijk Schoterpoort heeft de volgende maatregelen genomen en werkafspraken gemaakt om zeker te stellen dat patiëntgegevens zorgvuldig worden behandeld.

a) Alle medewerkers die patiëntgegevens verwerken of anderszins kennis nemen van patiëntgegevens zijn gehouden aan geheimhouding;

b) Patiëntgegevens worden niet langer bewaard dan nodig; medische gegevens worden in beginsel vijftien jaren bewaard, of zoveel langer als redelijkerwijs nodig om verantwoorde zorg te kunnen leveren. Medische dossiers van overleden patiënten worden nog vijftien jaar bewaard na de laatste wijziging in het dossier;

c) De ruimten waarin gegevens worden opgeslagen zijn niet vrij toegankelijk;

d) Patiënten worden bij de inschrijving bij de praktijk geïnformeerd over de gang van zaken betreffende de overdracht van het medisch dossier van de vorige huisarts; in de meeste gevallen wordt het dossier digitaal beveiligd verzonden;

e) Er is een grote afvalbak voor privacygevoelig materiaal, de inhoud wordt veilig vernietigd door firma Brantjes;

f) Er zijn opbergvakken voor spoedzaken per huisarts en per assistente, zodat er geen gegevens 's avonds op de bureaus blijven liggen; de kast met opbergvakken is buiten kantooruren gesloten met een cijferslot.

h) Alleen bevoegden hebben toegang tot de (digitale) gegevensbestanden van de praktijk; Jaarlijks wijzigen alle digitale wachtwoorden van alle medewerkers in de HOED omgeving, voor de inlog Zorgring en voor de Inlog Zorgdossier. Deze wachtwoorden voldoen aan de moderne eisen ((minimaal 1 hoofdletter, minimaal 1 kleine letter, minimaal 1 cijfer, minimaal 1 bijzonder teken, minimaal 8 tekens);

i) In Remote werken in praktijk omgeving gebeurt via VPN verbinding;

j) Virusscan NOD32 ESET endpoint antivirusscan is aanwezig;

k) Medische dossiers worden opgeslagen in ASDP omgeving bij Zorgring;

l) Een identieke server is als back- up ingericht;

m) De automatisering verloopt via Fersys . Fersys heeft geen toegang tot het patiëntendossier, wel tot de rest van de soft- en hardware. Fersys kan niet zelf inloggen in medische dossiers, dit is afgegrendeld;

n) Verbinding van het medisch dossier met de spoedpost: patiënten wordt om toestemming gevraagd middels een formulier, dit wordt hierna vernietigd;

o) Communicatie met de spoedpost wordt door de spoedpost beveiligd. Overdrachtgegevens van zorgpatiënten aan de spoedpost gebeurt via de website van de spoedpost via een beveiligde omgeving middels eigen inloggegevens en een eenmalig wachtwoord. Via dit netwerk is er ook een feedbackmodule voor patiënten die in de waarneming gezien zijn;

p) In mei 2016 is gestart met verwijzen en aanvragen van laboratorium en functie-onderzoek via de beveiligde applicatie Zorgdomein. In een minderheid van de gevallen zal de verwijsbrief nog meegegeven worden aan patiënt, opgestuurd worden per post of per e-mail worden verzonden aan de patiënt. In dit laatste geval wordt aangekaart dat 100% veiligheid per e-mail niet gegarandeerd is;

q) Specialistenbrieven en eerstelijnsberichten worden ontvangen via Edifact in zorgdossier en een kleiner deel wordt ontvangen via de post. Waarneemberichten van de HAP komen binnen via zorgdossier. Bij overlijden ontvangt de praktijk tevens een fax.

r) Sinds 2016 is er de mogelijkheid om via Doc-2-doc gegevens van de specialist in het Spaarne Gasthuis in te zien (lab, röntgen, medicatie, voorgeschiedenis, afspraken). Hiervoor moet een huisarts met een persoonsgebonden UZI-pas inloggen in een beveiligde omgeving. Het inzien van deze gegevens kan alleen nadat de patiënt specifiek voor het gebruik van Doc-2-doc schriftelijke toestemming heeft verleend.

Informatieveiligheid

Informatieverwerking door derden

De praktijk houdt een lijst bij van van organisaties waarmee zij patiëntengegevens deelt, zie het verwerkingsregister.

De praktijk sluit verwerkingsovereenkomsten met organisaties waarmee patiënteninformatie wordt gedeeld, zodat de organisatie in staat is om die patiënteninformatie te verwerken, zie alle verwerkingsovereenkomsten.

Beheer van databeveiligingsincidenten (datalek)

Beleid bij data veiligheidsincidenten (datalek)\

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Een datalek of zwakte in de databeveiliging dient gemeld te worden bij de dataverantwoordelijke/praktijkhouder.

Procedure bij een incident (datalek)

Indien er sprake is van een datalek, wordt door de dataverantwoordelijke het incidentenregistratieformulier ingevuld. Tevens wordt, aan de hand van de beslisboom melding datalek, besloten of het incident wel of niet gemeld moet worden bij de Autoriteit Persoonsgegevens (https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?0)

De dataverantwoordelijke zal de gedupeerde op de hoogte brengen van het incident.

Versie mei 2018