Beleid (AVG)
Fysiotherapie
Erik van Wegen

AVG onderdeel

Directieverklaring

De directie van Fysiotherapie Erik van Wegen is verantwoordelijk voor de veiligheid van de door haar verwerkte gegevens. Zij zorgt voor een privacy beleid of Information Security Management System (ISMS) dat passend is voor de organisatie. De doelstellingen van dat systeem stellen zeker dat de belangen van derden bij informatiebeveiliging voldoende worden beschermd. Zij verbindt zich eraan om het privacy beleid of ISMS continu te verbeteren en aan de (wettelijke) eisen te laten voldoen. Zij stelt voldoende middelen ter beschikking (binnen de mogelijkheden van de praktijk) om de veiligheid van gegevens te beschermen.

De directie van Fysiotherapie Erik van Wegen zorgt ervoor dat haar medewerkers zich bewust zijn van de vertrouwelijkheid van de (patiënten)-gegevens waarmee zij werkt en beschermt deze gegevens passend. Daarom werkt Fysiotherapie Erik van Wegen met een privacy beleid op basis van de Algemene Verordening Gegevensbescherming (AVG), of een ISMS op basis van de norm ISO27001, Informatiebeveiliging.

Het managementsysteem voor privacy- en informatiebeveiliging van Fysiotherapie Erik van Wegen beschermt de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie doordat zij een risicobeheerproces toepast, en geeft belanghebbenden het vertrouwen dat zij risico's adequaat beheert.

De directie van Fysiotherapie Erik van Wegen ondersteunt dit beleid, en voor de toepassing ervan stelt zij voldoende middelen ter beschikking (binnen de mogelijkheden van de praktijk). Het beleid van Fysiotherapie Erik van Wegen maakt zij blijvend bekend aan alle medewerkers van Fysiotherapie Erik van Wegen en relevante externe partijen.

De directie van Fysiotherapie Erik van Wegen zorgt ervoor dat het privacy beleid of ISMS op regelmatige wijze wordt gecontroleerd op zijn goede werking.

Werkingsgebied van het AVG privacybeleid en ISMS

Het werkingsgebied van het privacy beleid of ISMS van Fysiotherapie Erik van Wegen strekt zich uit tot de verantwoordelijkheden voor informatiebeveiliging van interne belanghebbenden (de bedrijfsgegevens van de praktijk zelf) en externe belanghebbenden (klanten, relaties, patiënten informatie).

Doel van gegevensverwerking

De gegevensverwerking door Fysiotherapie Erik van Wegen vindt plaats om de goede behandeling van patiënten mogelijk te maken.

Interne en externe communicatie over het AVG privacy beleid en ISMS

Intern besteedt de directie regelmatig aandacht aan het privacy beleid of ISMS van Fysiotherapie Erik van Wegen. Tijdens bijeenkomsten communiceert zij op regelmatige basis over dataveiligheids onderwerpen.

Fysiotherapie Erik van Wegen vermeldt extern in de uitingen en communicatie waar dat opportuun is dat Fysiotherapie Erik van Wegen via haar privacy beleid of ISMS werkt aan continue informatieveiligheid.

Eisen en verwachtingen van belanghebbenden

De belanghebbenden verwachten van Fysiotherapie Erik van Wegen dat zij gecontroleerd en op de meest veilige wijze met de (patiënten-) gegevens omgaat. Om die reden werkt Fysiotherapie Erik van Wegen volgens haar privacy beleid of ISMS. Dat privacy beleid of ISMS is gebaseerd op de wet AVG of ISO 27001 Informatieveiligheid. Het gehele privacy

beleid of ISMS is erop gericht blijvend de informatieveiligheid te waarborgen, te monitoren, corrigerende maatregelen te nemen en het privacy beleid of ISMS aan te passen indien nodig.

Privacy beleid (op basis van de AVG, voortvloeiend uit de Algemene Verordening Gegevensbescherming 2016/679)

Fysiotherapie Erik van Wegen gebruikt patiëntengegevens alleen voor het doel waarvoor de gegevens zijn opgeslagen. Fysiotherapie Erik van Wegen deelt patiëntengegevens niet met derden, tenzij dit voor het opslagdoel nodig is. Fysiotherapie Erik van Wegen bewaart patiëntengegevens niet langer dan nodig is op basis van het opslagdoel van de gegevens. Fysiotherapie Erik van Wegen houdt met alle mogelijke middelen en maatregelen patiëntengegevens veilig voor inzage van onbevoegden. Fysiotherapie Erik van Wegen vraagt toestemming aan de patiënten voor het opslaan van persoonsgegevens, als er *geen* behandelcontract gesloten is. Fysiotherapie Erik van Wegen informeert patiënten over de rechten van de patiënten ten aanzien van zijn persoonsgegevens. Fysiotherapie Erik van Wegen informeert haar patiënten over het doel van de verwerking van persoonsgegevens. Fysiotherapie Erik van Wegen informeert patiënten indien Fysiotherapie Erik van Wegen bijzondere handelingen met de persoonsgegevens gaat verrichten.

Risico-beoordeling (Data Protection Impact Assesment-DPIA)

Risico's bestaan in het door Fysiotherapie Erik van Wegen onbedoeld wijzigen of lekken of zoekraken van informatie waardoor schade ontstaat aan de externe belanghebbenden (patiënten en (oud-) patiënten van Fysiotherapie Erik van Wegen.

Tegen dit risico neemt Fysiotherapie Erik van Wegen de maatregelen in dit privacy beleid of ISMS, voert deze uit en beoordeelt deze op effectiviteit. De procedures van het privacy beleid of ISMS zijn onderwerp van continu onderzoek en verbetering. Alle medewerkers worden bij de veiligheids-procedures betrokken, op de wijzen als in dit privacy beleid of ISMS beschreven.

Procedure risico beoordeling

Fysiotherapie Erik van Wegen reduceert bovenstaande gevaren doordat zij werkt op basis van haar privacy beleid of ISMS. Bij iedere interne audit en management review wordt een risico-beoordeling dataveiligheid uitgevoerd.

Buiten het beheer van het privacy beleid of ISMS blijft een rest-risico bestaan. De bekende risico's voor Fysiotherapie Erik van Wegen worden via de interne audits en management reviews geanalyseerd. Maatregelen voor die risico's zijn in het privacy beleid of ISMS opgenomen en worden beheerd en uitgevoerd. Rest-risico's bestaan uit extreem wijzigende omstandigheden die Fysiotherapie Erik van Wegen niet voorziet. Die risico's acht Fysiotherapie Erik van Wegen onvermijdelijk. Na een onvoorzien incident wordt een nieuwe risico beoordeling uitgevoerd. Eventuele remedies neemt Fysiotherapie Erik van Wegen in het privacy beleid of ISMS op.

Creatie van AVG/ISMS documenten en procedures

De documenten voor het privacy beleid of ISMS worden voor Fysiotherapie Erik van Wegen gemaakt en beheerd door het dataveiligheidspakket van Waveland. Binnen Fysiotherapie Erik van Wegen zorgt de directie voor een verantwoordelijke voor het uitvoeren van de taken volgens het privacy beleid of ISMS.

Informatie aan betrokkenen (AVG)

Fysiotherapie Erik van Wegen informeert haar patiënten over de verwerking van persoonsgegevens en de rechten die de AVG aan de patiënten toekent.

Als patiënten **geen** 'behandelovereenkomst' sluiten met Fysiotherapie Erik van Wegen, vraagt Fysiotherapie Erik van Wegen uitdrukkelijke toestemming tot die verwerking.

Dit doet Fysiotherapie Erik van Wegen in overeenstemming met de Algemene Verordening Gegevensbescherming EU 2016/679 (AVG). Fysiotherapie Erik van Wegen gebruikt hiervoor haar document 'informatie aan cliënten'.

Bij de toepassing van de privacy wetgeving (AVG) houdt Fysiotherapie Erik van Wegen zich ook aan de WGBO, de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, Besluit elektronische gegevensverwerking in de zorg, en overige toepasselijke wetgeving. Deze wetten kunnen afwijken van de AVG.

Bij een toegekend verzoek tot verwijdering van persoongegevens zal Fysiotherapie Erik van Wegen de gegevens verwijderen of opslaan in een inactief archief waarmee het onzichtbaar is voor de gewone gebruiker binnen Fysiotherapie Erik van Wegen.
Fysiotherapie Erik van Wegen reageert op een verzoek zo spoedig mogelijk, maar in ieder geval binnen 3 maanden na de aanvraag.
Fysiotherapie Erik van Wegen heeft het formulier ‘Verzoek met betrekking tot persoonsgegevens’ beschikbaar voor patiënten die een verzoek willen doen aangaande hun persoonsgegevens.
In het geval Fysiotherapie Erik van Wegen een verzoek over de persoonsgegevens afwijst, informeert Fysiotherapie Erik van Wegen de patiënten over de redenen voor de afwijzing.

Verwerkingsregister en informatie classificatie (AVG)

AVG onderdeel

Informatie classificatie

Fysiotherapie Erik van Wegen classificeert informatie met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging en de bewaartermijn. Fysiotherapie Erik van Wegen maakt onderscheid tussen openbare informatie en gevoelige informatie.

Informatie over de behandeling van patiënten van Fysiotherapie Erik van Wegen is altijd gevoelige informatie.

Informatie over medewerkers van Fysiotherapie Erik van Wegen is altijd gevoelige informatie.
Medische informatie is altijd gevoelige informatie.

Bedrijfsmiddelen (waaronder ook 'data' behoort) worden behandeld in overeenstemming met het informatieclassificatieschema dat is vastgesteld door Fysiotherapie Erik van Wegen.

Fysiotherapie Erik van Wegen bewaart de (persoons) gegevens in het behandeldossier volgens de wettelijke bewaartermijn van de WGBO. Fysiotherapie Erik van Wegen vernietigt gegevens na het verstrijken van de wettelijke bewaartermijn.

Fysiotherapie Erik van Wegen is in staat de volgende acties uit te voeren met haar informatiepakket:

-Gegevens laten **inzien** door onze patiënten. Alleen de gegevens van de bewuste patiënten mogen dan inzichtelijk zijn. (de patiënten mogen geen wijzigingen in ons systeem kunnen aanbrengen tijdens het inzien.)
-**Correcties** (en wijzigingen) aanbrengen, alleen mogelijk door een geautoriseerde verwerker van Fysiotherapie Erik van Wegen.
-Gegevens van één persoon **overdragen.**
-**Verwijderen** van alle, of een deel van de gegevens van één persoon (een persoon heeft het recht om 'vergeten te worden' op basis van de AVG, dit recht wordt opzij gezet door de WGBO bepalingen). Fysiotherapie Erik van Wegen beoordeelt het verzoek met in achtneming van de eisen van de WGBO. Als er goede redenen zijn om het verzoek af

te wijzen, legt Fysiotherapie Erik van Wegen dit vast in het patiëntendossier en brengt Fysiotherapie Erik van Wegen de patiënten van de beslissing op de hoogte.

Verwerkingsregister van Fysiotherapie Erik van Wegen:

Per verwerkingsactiviteit staan mogelijk de volgende gegevens geregistreerd:

-Naam van de dataverantwoordelijke is vastgelegd bij onderdeel 'praktijksamenstelling'
-Fysiotherapie Erik van Wegen slaat de noodzakelijke gegevens van medewerkers op in het personeelsdossier.
-Fysiotherapie Erik van Wegen slaat de volgende data van patiënten op:
-NAW gegevens,
-BSN nummer,
-Geslacht,
-Leeftijd,
-Telefoonnummer,
-Emailadres van patiënten,
-Medische gegevens, het gehele patiëntendossier,
-(Rontgen) -foto's gericht op de medische behandeling,
- Laboratorium uitslagen,
- Sexueel verleden, indien dat voor het verlenen van de zorg nodig en/of relevant is,
- Etnische afkomst, indien dat voor het verlenen van de zorg nodig en/of relevant is,
- Godsdienst, indien dat voor het verlenen van de zorg nodig en/of relevant is,
- Opleidingsniveau, indien dat voor het verlenen van de zorg relevant is.

-Medische gegevens van Fysiotherapie Erik van Wegen zijn 'bijzondere gegevens' volgens de AVG wetgeving.
-Informatie wordt opgeslagen om behandeling van de patiënten mogelijk te maken.
-Informatie wordt verwerkt door behandelaars en hun assistenten en praktijkondersteunende diensten.
-Informatie wordt verwerkt van patiënten die de Fysiotherapie Erik van Wegen behandelt.
-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 patiënten.
-De informatie wordt uitgewisseld met andere behandelaars die nodig zijn voor de goede behandeling.
-Informatie wordt uitgewisseld met verzekeraars of hun vertegenwoordigers (Vecozo). Als die niet gebeurt op grond van een wettelijke verplichting, vraagt Fysiotherapie Erik van Wegen hiervoor toestemming aan de patiënten.
-Fysiotherapie Erik van Wegen verstrekt geen Informatie aan buitenlandse organisaties, tenzij de goede behandeling dit nodig maakt.
-De bewaartermijn is zo lang als de informatie nodig is voor de goede behandeling, met in achtneming van de WGBO.
-De beveiligingsmaatregelen zijn in de afdeling van het DataVeiligheidsportaal te vinden, in de AVG- of ISMS vastlegging van Fysiotherapie Erik van Wegen.

Per verwerker: (daaronder verstaat Fysiotherapie Erik van Wegen onderaannemers van Fysiotherapie Erik van Wegen die gevraagd worden een handeling uit te voeren met persoons***gegevens*** in opdracht van Fysiotherapie Erik van Wegen. Daaronder vallen *niet* de zorgverleners die onderdeel uitmaken van de medische behandeling. Die behandelaars zijn zelf verantwoordelijk voor de beveiliging van de privacy van de patiënten.

-Informatie wordt door derden verwerkt (verwerkers) met als doel de goede behandeling van patiënten.

-Fysiotherapie Erik van Wegen deelt persoonsgegevens van medewerkers met derden als dat nodig is voor de goede uitvoering van het arbeidscontract.
-Fysiotherapie Erik van Wegen sluit met verwerkers een verwerkingcontract. Daarin staan de voorwaarden voor de verwerking.

De categorieën van het verwerkingsregister van Fysiotherapie Erik van Wegen zijn in haar dataveiligheids portaal te vinden onder 'beheer van bedrijfsmiddelen'.

Andere persoonsgegevens die wij opslaan:
Arbeids en activiteitengegevens gezondheidsgegevens welke worden aangegeven in het intake formulier

---

Beleid bewustwording (AVG)

AVG onderdeel

Het contract van iedere medewerker bij Fysiotherapie Erik van Wegen bevat bepalingen over geheimhouding van gegevens en de verantwoordelijkheid om veilig met data om te gaan.

Om dit te onderstrepen organiseert Fysiotherapie Erik van Wegen regelmatig, minimaal 4 keer per jaar via bewustwordingssessies en interne audits over dataveiligheid, samen met alle medewerkers van Fysiotherapie Erik van Wegen. Ontwikkelingen op het gebied van dataveiligheid (breed) worden verspreid en besproken binnen Fysiotherapie Erik van Wegen.

Fysiotherapie Erik van Wegen plant regelmatig bijeenkomsten waarin het privacy beleid en/of ISMS en dataveiligheid worden besproken.

Toegangsbeveiliging van data (AVG)

AVG onderdeel

Autorisatie matrix

Toegang tot informatie verstrekt Fysiotherapie Erik van Wegen op basis van de directe taken en bezigheden van betreffende medewerker. Dit wordt weergegeven in de autorisatiematrix van de verschillende informatiesystemen.

De toegang tot informatie van Fysiotherapie Erik van Wegen is te vinden in de rollen en/of profielen in het informatiepakket dat Fysiotherapie Erik van Wegen gebruikt.

Wachtwoorden

De toegang tot het (draadloze) netwerk en netwerkdiensten wordt afgedwongen met persoonlijke wachtwoorden.

Informatiebeveiliging met derden en in leveranciersrelaties (AVG)

AVG onderdeel

Fysiotherapie Erik van Wegen houdt een lijst bij van categorieën van organisaties waarmee zij patiëntengegevens deelt. (zie het verwerkingsregister afd. 3/7 - 19/37).

Fysiotherapie Erik van Wegen sluit verwerkingsovereenkomsten met organisaties waarmee zij patiënteninformatie deelt om die patiëntengegevens te verwerken. (Voorbeeld). Fysiotherapie Erik van Wegen vult haar verwerkersovereenkomst aan met het contract waarin de opdracht aan de verwerker nauwkeurig wordt omschreven. Indien Fysiotherapie Erik van Wegen dit wenst voegt zij beide overeenkomsten samen.

Fysiotherapie Erik van Wegen houdt een leverancierslijst bij van leveranciers die mogelijk patiëntengegevens van de praktijk kunnen inzien, en met welke organisaties zij een verwerkerscontract heeft gesloten. Fysiotherapie Erik van Wegen houdt die leverancierslijst actueel. De betreffende leverancier tekent de verwerkersovereenkomst (daarin is geheimhouding opgenomen)

Ondanks deze verwerkersovereenkomst, deelt Fysiotherapie Erik van Wegen niet meer informatie dan strikt noodzakelijk is om gevraagde dienst/service/behandeling uit te voeren.

Fysiotherapie Erik van Wegen sluit een geheimhoudingsverklaring met personen die onbedoeld persoonsgegevens kunnen inzien. Dit kan in de serviceovereenkomst staan, of in een aparte geheimhoudingsverklaring.

Beheer van informatiebeveiligingsincidenten (datalek) (AVG)

AVG onderdeel

Beleid bij data veiligheidsincidenten (datalek)
Een datalek (of: data incident) is voor Fysiotherapie Erik van Wegen: iedere inbreuk op de dataveiligheid die per ongeluk of op onrechtmatige wijze leidt tot:
• vernietiging van data of informatie,
•verlies van persoonsgegevens,
•wijziging van persoonsgegevens,
•ongeoorloofde verstrekking van persoonsgegevens,
•ongeoorloofde toegang tot opgeslagen persoonsgegevens,
•ongeoorloofde toegang tot doorgezonden persoonsgegevens.

Een datalek ontstaat onder andere als Fysiotherapie Erik van Wegen het slachtoffer wordt van ransomware of een andere vorm van kwaadwillige hacking.

In het geval dat zich een dataveiligheids incident voordoet of een zwakte in de databeveiliging geconstateerd wordt door een medewerker, meldt hij dit zo spoedig mogelijk bij zijn of haar leidinggevende en de verantwoordelijke voor databeveiliging van Fysiotherapie Erik van Wegen.

Na een incident analyseert Fysiotherapie Erik van Wegen de oorzaak, de aanpak en de mogelijkheden om een dergelijk incident te voorkomen. Zij legt haar bevindingen vast in het formulier 'dataveiligheidsincident'. De maatregelen *ter voorkoming* van het incident worden na invoering geëvalueerd.