therapieland

Privacy & Security 2020

Therapieland BV | ISO 27001 en NEN 7510

Privacy & Security 2020

Therapieland BV | ISO 27001 en NEN 7510

Therapieland & Gezondeboel

Security & privacy

Januari 2020

versie 1

Auteur: Marjoleine Konersmann

Introductie

Over Therapieland

Therapieland ontwikkelt online e-health-applicaties voor de ggz, de bedrijfsgezondheidszorg, de huisartsenzorg, ziekenhuizen, wijkteams en voor mensen die zelf aan de slag willen.

Onze gebruikers vertrouwen ons met de gegevens die zij invoeren in het platform. Wij zijn ons bewust van de verantwoordelijkheid die daarmee gepaard gaat en daarom willen wij een zo veilig mogelijk platform bieden voor onze gebruikers. Wij doen dit door de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te waarborgen. Deze folder licht toe hoe we dat hebben vastgelegd.

Wij spreken in deze folder over Therapieland. Hieronder vallen al onze applicaties (Virtual Reality, vragenlijstportaal en het online platform met modules) en ook het label Gezondeboel valt hieronder. Verder spreken wij van gebruikers. Dit zijn de mensen die een account hebben waarmee zij kunnen inloggen in het platform. Denk hierbij aan behandelaren en aan cliënten/patiënten.

ISO 27001 en NEN 7510

Therapieland is ISO 27001 en NEN 7510 gecertificeerd. Dat betekent dat wij ons jaarlijks door een onafhankelijke partij laat auditen op het informatiebeveiligingsbeleid en de beheersmaatregelen die daarbij horen.

Scope van ISMS

Het ontwikkelen en aanbieden van de online platformen van Therapieland met applicaties voor psychologische ondersteuning die toegankelijk is voor gebruikers die kunnen inloggen met hun persoonlijke account, het verzorgen van de implementatie bij de afnemer en het leveren van helpdesk & support, in overeenstemming met de verklaring van toepasselijkheid.

Databeheer & hosting

Wij hebben ons databeheer en hosting uitbesteed aan externe partijen. De data van Therapieland wordt extern beheerd bij een ISO 27001 gecertificeerd datacentrum gevestigd in Amsterdam en Delft. Onze hostingpartij is ISO 27001 & NEN 7510 gecertificeerd en is gevestigd in Leiden.

Bewustzijn & opleiding onder de medewerkers van Therapieland

We hebben bij Therapieland meerdere beheersmaatregelen aangaande de medewerkers. Denk hierbij aan een disciplinaire procedure, toegangsbeveiliging, maatregelen rondom thuis en extern werken. Een greep van deze beheersmaatregelen wordt hieronder verder toegelicht.

De medewerkers van Therapieland ondertekenen een geheimhoudingsovereenkomst. Zij mogen gegevens van gebruikers niet inzien, bewerken, delen en/of verwijderen tenzij het nodig is voor het kunnen uitvoeren van hun functie en/of het kunnen beantwoorden van een helpdeskticket.
Daarnaast ontvangen medewerkers twee trainingen over informatiebeveiliging. Zij leren hoe zij incidenten kunnen voorkomen en hoe zij informatiebeveiliging kunnen toepassen in hun dagelijkse werkzaamheden.

De acties van medewerkers in ons systeem worden gelogd en gecheckt op opvallendheden door de security officer.

Protocollen datalek & incidenten

Therapieland heeft protocollen voor het geval dat er een incident plaatsvindt. Medewerkers zijn getraind incidenten te herkennen en deze te rapporteren bij de juiste leidinggevende. De incidenten worden regelmatig geëvalueerd zodat er stappen kunnen worden ondernomen om soortgelijke incidenten in de toekomst tegen te kunnen gaan. Alle incidentmeldingen worden beheerd en bewaard.

Pentesten

Jaarlijks vinden er pentesten plaats waarbij Therapieland zich door een onafhankelijke partij laat testen op technische kwetsbaarheden. De test detecteert kwaadaardige software, zwakke plekken in het platform en controleert de infrastructuur en netwerken op kwetsbaarheden.

Wetgeving

Therapieland is AVG-compliant en werkt nauw samen met een extern juridisch adviesbureau om aan nieuwe en bestaande wetten te voldoen.

Therapieland sluit met al zijn klanten een verwerkingsovereenkomst af. Ook worden er verwerkingsovereenkomsten afgesloten met externe partijen indien nodig. Zo hebben wij met ons datacentrum en hostingpartij een verwerkersovereenkomst afgesloten. Er is een helder beschreven privacy statement waar de rechten van de gebruiker en hoe hij/zij deze kan inwilligen wordt beschreven.

Verder hebben wij technische maatregelen ingeregeld om aan de AVG te kunnen voldoen. Gebruikers kunnen bijvoorbeeld zelf hun account verwijderen, gebruikers kunnen logdata opvragen, wij verwerken buiten de huisartsenzorg om geen BSN en geboortedatum, inloggen met tweefactorauthenticatie is mogelijk voor onze gebruikers.

Therapieland beheert een lijst met subverwerkers die opgevraagd kan worden. Op dit moment heeft Therapieland alleen het extern datacentrum als subverwerker.

Verificatie & toegang

Je kunt bij Therapieland maar één account hebben per e-mailadres. Het e-mailadres wordt geverifieerd door middel van een activatie- of uitnodigingse-mail. Inloggen moeten gebruikers met hun e-mailadres en sterk wachtwoord (minimaal acht tekens en een bijzonder teken wordt systematisch afgedwongen). Gebruikersgegevens worden gescheiden opgeslagen. Medewerkers van Therapieland loggen in met tweefactorauthenticatie. Deze functionaliteit is ook beschikbaar voor onze gebruikers.

Gegevens die worden verwerkt

Soorten gegevens die worden verwerkt van zelfhulpgebruikers:

- E-mailadres
- Nickname
- Geslacht
- Bezoekgedrag website
- IP-adres
- Gegevens ingevoerd in het platform (opdrachten, berichten, vragenlijsten)

Soorten gegevens die worden verwerkt met tussenkomst van een behandelaar:

- E-mailadres
- Naam en achternaam
- Nickname
- Geslacht
- Bezoekgedrag website
- IP-adres
- Gegevens ingevoerd in het platform (opdrachten, berichten, vragenlijsten)
- BSN (alleen met de tussenkomst van een huisartsenpraktijk of als de behandelaar deze heeft ingevoerd)
- Geboortedatum (alleen met de tussenkomst van een huisartsenpraktijk of als de behandelaar deze heeft ingevoerd)

De doeleinden van gegevensverwerking:

- het verlenen van toegang tot onze website;
- het opnemen van contact met cliënten, als zij daarom verzoeken;
- het gebruik maken van de algemene functionaliteiten op onze website;
- het verkrijgen van inzicht in het gebruik van onze website;
- het aanbieden van behandelingen via ons platform;
- het doen van analyses en metingen;
- het doen van wetenschappelijk onderzoek (mits hier apart toestemming voor is gegeven).

Bewaartermijn gegevens

Therapieland hanteert een bewaartermijn van twintig jaar (gebaseerd op de dossierplicht van de WGBO). Echter, organisaties kunnen zelf hun eigen bewaartermijn bepalen en dossiers kunnen verwijderd worden.

Analyses en metingen

We maken gebruik van gegevens om analyses en metingen te doen. Dit helpt ons meer inzicht krijgen in het gebruik van onze website en het platform. Wanneer wij bijvoorbeeld zien dat bepaalde stappen van een programma vaker of minder vaak worden bezocht kunnen wij aanpassingen maken binnen het programma. Dit helpt ons het programma te verbeteren en beter aan te laten sluiten op onze gebruikers. Hiermee hopen we een platform te kunnen aanbieden dat u als prettig ervaart en ondersteunt in uw behoefte. Ook maken wij gebruik van metingen om persoonlijke aanbevelingen te kunnen doen.

Het platform bevat een aantal vragenlijsten. De ingevulde gegevens van de vragenlijsten worden gebruikt ten behoeve van analyses en metingen en worden door ons strikt vertrouwelijk behandeld. Er wordt nooit op individueel niveau gerapporteerd. Gegevens worden nooit aan derden doorgegeven tenzij de gebruiker daar expliciet toestemming voor heeft gegeven.

Wetenschappelijk onderzoek

In samenwerking met universiteiten, hogescholen en kennisinstituten doet Therapieland wetenschappelijk onderzoek met als doel kennis op te doen over het gebruik, de werking en waardering van e-health. Binnen deze samenwerking leren wij samen voor wie e-health kan helpen en welke elementen daarin belangrijk zijn. Opgedane kennis kan worden gepubliceerd in (wetenschappelijke) artikelen om de zorg te verbeteren. Gebruikers kunnen zelf aangeven of zij hieraan willen meedoen. Ook kunnen zij hun toestemming op een later moment weer intrekken. Wij gebruiken uitsluitend geanonimiseerde gegevens. Wanneer wij gegevens delen met samenwerkende partijen zullen wij deze gegevens van tevoren anonimiseren.

Rollen, rechten en verantwoordelijkheden

We hebben een uitgebreid rollen- en rechtenmodel en de daarbij horende toegangsrechten.

Fysieke beveiliging

Therapieland heeft fysieke beveiligingsmaatregelen ingericht. Ruimtes worden afgesloten en er zitten sloten/toegangscodes op ramen en deuren. Het pand wordt afgeschermd met een hek.

Het datacentrum heeft fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten. Ook wordt de apparatuur beschermt tegen stroomuitval en andere storingen.
Het datacenter wordt 24/7 beveiligd. Zowel op het netwerk als op het terrein zelf.
Overal wordt HTTPS gebruikt en er is dubbele uitvoeringen van voedings- en telecommunicatiekabels, zodat er geen single point of failure is.

IT & beveiligd ontwikkelen

Therapieland hanteert een 'IT security policy' waar beveiligd ontwikkelen centraal staat. Wij hebben een ontwikkel-, test- acceptatie- en productieomgeving. Onze platformen zijn beveiligd met een SSL-certificaat en het platform is encrypted. De broncode is afgesloten en er zijn protocollen voor de releases, zodat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie wordt beheerst. De toegangen tot data of systemen hebben we beveiligd vanuit het Principle of Least Privilege (PoLP). Tot slot werkt het ontwikkelteam vanuit strenge ontwikkelprincipes, waardoor technisch falen zoveel mogelijk wordt voorkomen.

Logging

Onze logbestanden worden beschermd en kunnen niet bewerkt worden. Logs kunnen opgevraagd worden.

Netwerken

De netwerken van Therapieland worden beveiligd en gescheiden van elkaar. Medewerkers mogen extern alleen op hun eigen hotspot werken.

Backups

Therapieland doen zeer periodiek backups. Deze backups staan on- en offsite om het risico van data-loss te verkleinen. Om de backups te beveiligen, zijn ze geëncrypt opgeslagen. Er is een proces ingeregeld en getest voor disaster recovery.

www.therapieland.nl

Nieuwendammerdijk 528 | 1023 BX Amsterdam

T 020 771 28 48 | info@therapieland.nl