PodoFile
Software voor pedicure en podoloog

BeautyFile
Software voor beauty- en massagesalons

Uw praktijk en de Wet Bescherming Persoonsgegevens

1 INHOUD

2 INLEIDING

Iedereen die beroepshalve een patiëntenadministratie bijhoudt, of dat nu op papier is of door middel van een programma of een on-line systeem, krijgt te maken met de Wet Bescherming Persoonsgegevens.

Wist u dat u verplicht bent u aan te melden bij de Autoriteit Persoonsgegevens (AP), maar dat u in de meeste gevallen vrijstelling kunt krijgen?

Wist u dat u alles wat redelijk is moet doen om te zorgen dat de persoonsgegevens niet in verkeerde handen kunnen vallen?

Wist u dat als dit toch gebeurt u verplicht bent dit te melden aan de AP?

Wilt uw weten in hoeverre uw gegevens in PodoFile en BeautyFile veilig zijn?

Op deze vragen geeft dit artikel een antwoord.

3 De Wet Bescherming Persoonsgegevens

De Wet Bescherming Persoonsgegevens (WBP) beschermt de privacy van een ieder. PodoFile en BeautyFile zijn gedigitaliseerde systemen waarmee persoonsgegevens kunnen worden verwerkt. De WBP noemt een aantal handelingen met betrekking tot persoonsgegevens die worden aangeduid als verwerking. Bijvoorbeeld het verzamelen, vastleggen en ordenen; het bewaren en wijzigen; het opvragen, raadplegen en gebruiken; het verspreiden of in andere vorm ter beschikking stellen van deze gegevens.

4 Meldplicht verwerking persoonsgegevens

De WBP beoogt een zo klein mogelijke inbreuk van de privacy van personen. Gegevens mogen daarom alleen worden verwerkt voor een bepaald doel en in overeenstemming met de grondslag van de wet. In beginsel dient de verwerking te worden aangemeld bij de Autoriteit Persoonsgegevens (AP). Echter op grond van het vrijstellingsbesluit Individuele gezondheidszorg (Handreiking Vrijstellingsbesluit Paragraaf 4. Zorg en welzijn: Vrijstelling 14. (Artikel 16 Vrijstellingsbesluit)) zijn zorgverleners die gebruik maken van genoemde programma's in de meeste gevallen vrijgesteld van deze verplichting. Maar niet in alle gevallen. Er dient bijvoorbeeld sprake te zijn van één verantwoordelijke. De beoordeling of in uw geval het vrijstellingsbesluit van toepassing is, is uw eigen verantwoordelijkheid. Bij twijfel is het aan te raden zich aan te melden; zie de weblink die hieronder is vermeld.

5 Beveiligingsmaatregelen

Tevens is het noodzakelijk dat u voldoende maatregelen neemt om verlies van gegevens of het gebruik van gegevens door onbevoegden te voorkomen. Hieronder vallen algemene maatregelen zoals onder meer de toegang tot de ruimte waar de PC zich bevindt en het zoveel mogelijk beperken van het aantal medewerkers dat de gegevens kan inzien.
In het programma zelf zijn de volgende maatregelen genomen om u in staat te stellen uw gegevens optimaal te beveiligen.

1. Toegankelijkheid tot het gebruik van het programma op basis van wachtwoorden. Het gebruikmaken van deze mogelijkheid wordt ten sterkste aanbevolen, maar is uw eigen verantwoordelijkheid. Het communiceren met Vecozo-diensten is niet mogelijk zonder het gebruik van een voldoende sterk wachtwoord.
2. Voor de toegang tot Vecozo-diensten is het bovendien noodzakelijk om een systeemcertificaat te installeren op uw systeem. Dit betekent dat, in combinatie met het algemene wachtwoord, er een vorm van tweetraps authenticatie is gerealiseerd.
3. De betreffende opgeslagen gegevens zijn versleuteld.
4. De gegevens worden uitsluitend opgeslagen op uw eigen systeem, te weten 1) de harde schijf van uw computer; 2) een door u te bepalen locatie zoals een externe harde schijf, USB-stick, NAS of uw eigen account bij een clouddienst.
5. De toegang tot uw systeem en het gebruik van de gegevens worden gelogd.
6. Het systeem biedt de mogelijkheid om gegevens regelmatig op te slaan in versleutelde backup-bestanden welke uitsluitend met behulp van het programma kunnen worden geopend.

Zorg verder voor een goede, up-to-date, beveiliging (anti-virus, firewall, antimalware). Zorg ook dat uw netwerk niet toegankelijk is voor derden. Gebruik geen operating systeem dat niet meer wordt

ondersteund door de fabrikant. De gegevens mogen niet worden opgeslagen buiten de EU. Dit laatste beperkt vooralsnog de keuze van clouddiensten voor de opslag van de gegevens.

6 MELDPLICHT DATALEKKEN

Mocht u onverhoopt toch gegevens kwijtraken, of wanneer het vermoeden bestaat dat derden uw gegevens hebben gekopieerd, dan bent u verplicht dit te melden aan de Autoriteit Persoonsgegevens. Enkele voorbeelden: u verliest een USB-stick waarop backups staan; uw computer wordt gestolen; uw computer wordt gehackt; uw cloud account dat u gebruikt om uw gegevens op te slaan wordt gehackt.

7 MEER INFORMATIE

Voor meer informatie: https://autoriteitpersoonsgegevens.nl/nl