Hoe het begon

Diasoft is in 1991 opgericht door Cablon Medical en Stichting Thuisdialyse. De dialyseprofessionals waren op zoek naar een patiëntendossier en de twee bedrijven gingen daarmee aan de slag. Dat was het begin van Diasoft. We begonnen als stichting, en werden later Diasoft BV.

Voor 1995 installeerde Diasoft de eerste Diamant. Bijna 10 jaar later werd de Diamant Windows versie geïnstalleerd. Nu, meer dan 15 jaar na die installatie, is Diasoft actief in 16 landen en 4 continenten. En we groeien nog steeds. Onze droom is honderdduizenden nierpatiënten over de hele wereld te helpen bij het verzamelen en hergebruiken van medische gegevens. Op die manier willen we de kwaliteit van hun behandeling verbeteren.

Onze missie

Onze missie is om professionals in de gezondheidszorg te faciliteren en de veiligheid van patiënten te verhogen door een geavanceerd en veilig medisch hulpmiddel te creëren en te onderhouden dat de zorg voor nierpatiënten ondersteunt.

Onze kernwaarden

- Respect voor elk individu
- Focus op veiligheid en privacy
- Professioneel en onafhankelijk in het omgaan met gegevens
- Toegewijd aan het verbeteren van de kwaliteit van de behandeling
- Gemakkelijk te benaderen

Ons team

Diasoft heeft als doel gezondheidszorg professionals te helpen om de beste ervaring te krijgen met Diamant. Om dit te bereiken, bestaat ons team uit gespecialiseerde technici. Nefrologen, verpleegkundigen, diëtisten, patiënten en verdelers kunnen gebruik maken van de expertise van dit toegewijde team. De expertise van Diasoft is markt gedreven. Diasoft wordt echter beheerd door en voor de Diamantgebruikers. Wij werken voortdurend aan de verbetering van onze software. Op deze manier wordt de veiligheid van het systeem gegarandeerd. Klanten beschikken over een compleet softwarepakket en hoeven zich geen zorgen te maken over moeilijke procedures.

Onze veiligheidseisen

Het doel van Informatiebeveiliging is het waarborgen van de bedrijfscontinuïteit en het minimaliseren van bedrijfsschade door het voorkomen en minimaliseren van de impact van beveiligingsincidenten. Met name moeten informatiemiddelen worden beschermd om te zorgen voor:

1. Vertrouwelijkheid, d.w.z. bescherming tegen ongeoorloofde openbaarmaking
2. Integriteit, d.w.z. bescherming tegen ongeoorloofde of accidentele wijziging
3. Beschikbaarheid waar en wanneer nodig voor het realiseren van de bedrijfsdoelstellingen.

Verantwoordelijkheden:

1. De directie heeft dit Informatiebeveiligingsbeleid goedgekeurd.

2. De dagelijkse verantwoordelijkheid voor en de contacten met externe organisaties voor de naleving van de wettelijke eisen, met inbegrip van de bescherming van gegevens, berusten bij de Information Security Officer en Privacy Officer.

3. Alle werknemers of dienstverleners namens de organisatie hebben de plicht om de middelen, inclusief locaties, hardware, software, systemen of informatie, die zij onder hun hoede hebben, te beschermen en elke vermoede inbreuk op de beveiliging onmiddellijk te melden.

4. Het naleven van informatiebeveiligingsprocedures zoals uiteengezet in de beleids- en richtlijnstukken wordt geaccepteerd als onderdeel van de standaardwerkwijzen binnen de organisatie. Niet-naleving leidt tot disciplinaire maatregelen.

5. Aan alle wettelijke en reglementaire vereisten wordt voldaan en regelmatig op wijzigingen gecontroleerd.

6. Er is een bedrijfscontinuïteitsplan. Dit wordt onderhouden, getest en regelmatig herzien.

7. Dit informatiebeveiligingsbeleid wordt regelmatig herzien en kan door de Information Security Officer worden gewijzigd om de blijvende levensvatbaarheid, toepasbaarheid en naleving van de wetgeving te waarborgen en om de informatiebeveiliging systemen voortdurend te verbeteren.

8. De directie stuurt erop aan dat er wordt voldaan aan de geldende wet- en regelgeving en dat middels het Informatiebeveiligingsmanagementsysteem continue verbetering wordt bewerkstelligd binnen de organisatie.