



Training

Bescherming Patiëntgegevens



Training Bescherming Patiëntgegevens

Doel

De training is gericht op het beschermen van de patiëntgegevens en op toepassing hiervan in de dagelijkse praktijk van de zorg.

Verlies of verminking van patiëntgegevens heeft een negatieve invloed op het zorgtraject. Als de patiënt het gevoel heeft dat zijn gegevens bij de zorgverlener in goede handen zijn, heeft dat een directe invloed op de vertrouwensrelatie.

Naast het zorginhoudelijke, juridische en financiële belang is bescherming van patiëntgegevens eigenlijk de morele en ethische verantwoordelijkheid van elke zorgprofessional.

Daarom is bewustwording van de zorgverlener over het beschermen van zijn patiëntgegevens en de praktische invulling hiervan essentieel voor de veiligheid van de patiënt.

Doelgroep

De training is gericht op eerstelijnsgezondheidszorg.

Benadering

De training concentreert zich op de dagelijkse praktijk en op de bedrijfsvoering die het werkproces ondersteunt. De training is praktisch gericht, wat resulteert in een interactieve aanpak met nadruk op het uitwisselen van kennis en ervaringen. In de training leren de trainees een optimale balans te vinden tussen het afschermen en het ter beschikking stellen van informatie over hun patiënten, ieder in zijn eigen praktijksituatie.

Onderwerpen

- ★ Informatiehuishouding als een te onderscheiden aspect in de bedrijfsvoering.
- ★ Goed beheerd zorgsysteem (GBZ).
- ★ Elektronisch patiënten dossier (EPD), zowel per praktijk, samenwerkingsverband, ASP, regionaal en landelijk.
- ★ De drie aspecten van informatiebeveiliging; beschikbaarheid, integriteit en vertrouwelijkheid.
- ★ De Praktijkwijzer Informatiebeveiliging van het NHG.
- ★ De ethische verantwoordelijkheid van een zorgverlener.
- ★ Relevante wetten en richtlijnen zoals de norm NEN 7510, de norm voor informatiebeveiliging in de zorg.
- ★ Kwaliteitscirkel.
- ★ Autorisatie.
- ★ Gedrag en bedrijfsvoering.

Programma

De training duurt vier uur, onderbroken door een half uur pauze. De nadruk ligt op de eigen praktijk (bedrijfsvoering en gedrag), op het uitwisselen van ervaringen en ideeën en op concrete verbeteringen om in de eigen praktijk toe te passen.

Achtereenvolgens worden de volgende onderwerpen behandeld.

- ★ De stand van de informatiebeveiliging in de eigen praktijk.
- ★ Patiëntveiligheid en informatiebeveiliging.
- ★ Een kort theoretisch gedeelte: Wat is informatiebeveiliging en hoe implementeer ik het in de eigen praktijk.
- ★ Een checklist voor informatiebeveiliging, in lijn met de te verschijnen Praktijkwijzer Informatiebeveiliging van het NHG, wordt toegepast.
- ★ Regionale EPD's en het landelijk EPD.
- ★ Gegevensoverdracht bij waarneming buiten kantooruren.
- ★ Een verbeterplan voor de eigen praktijk.

Na afloop van de cursus is er de mogelijkheid om enige telefonische ondersteuning in de praktijk te krijgen. Dit wordt gezien als onderdeel van de training.

De training wordt begeleid door twee docenten met ruime ervaring in de informatiebeveiliging in de gezondheidszorg.

Resultaat van de training

Aan het eind van de training kent de zorgverlener de sterke en zwakke punten van de eigen informatiebeveiliging en is in staat om gerichte en passende maatregelen te nemen.

De zorgverlener:

- ★ Kan richting geven aan de eigen praktijk in het brede gebied van de informatiebeveiliging.
- ★ Kan de aspecten van het beschermen van patiëntgegevens benoemen.
- ★ Kan zijn/haar eigen bescherming van de patiëntgegevens beoordelen.
- ★ Heeft kennis gemaakt met diverse praktische stappen die het beschermen van de patiëntgegevens vergemakkelijken.
- ★ Heeft kennis van de relevante wetten en normen.
- ★ Heeft kennis gemaakt met GBZ en de oplossingen die nu beschikbaar zijn.
- ★ Heeft kennis en ervaringen uitgewisseld met andere zorgverleners.

Voor meer informatie

Telefoon: 06 54 28 75 82 (Med. Drs. Hossein Seyed Nabavi) of
06 21 70 02 85 (Drs. Jaap van der Kamp CISSP)

Website: www.ibgz.nl

Inschrijving

wordt in principe geregeld via de eerstelijns nascholing in de regio of via uw beroepsvereniging. Wilt u als individu deelnemen, dan kunt u gebruik maken van ons contactformulier op <http://www.ibgz.nl/contact.html>



Informatiebeveiliging
Gezondheidszorg

Medio 2007 is in Amsterdam de Stichting Informatiebeveiliging Gezondheidszorg (Stichting IBGZ) opgericht.

Stichting IBGZ stelt zich tot taak om informatiebeveiliging in de gezondheidszorg in kaart te brengen en haar invloed op de patiëntveiligheid te onderzoeken.

Daarnaast bevordert IBGZ het beveiligingsbewustzijn bij de mensen die werkzaam zijn in de gezondheidszorg en de daaraan gerelateerde bedrijfstakken.

Contact

Stichting Informatiebeveiliging Gezondheidszorg (Stichting IBGZ)

Adres: Nannie van Wehlstraat 12
1064 MN Amsterdam

Telefoon: 06 54 28 75 82

Email: ibgz@ibgz.nl

Website: www.ibgz.nl