3. Privacy en informatieveiligheid

Voor verschillende doeleinden legt Fivoor persoonsgegevens vast van patiënten en van medewerkers. Dit betreffen privacygevoelige gegevens. Het Privacyreglement van Fivoor geeft een kader om de verwerking van deze persoonsgegevens op een (juridisch) juiste en inzichtelijke wijze te laten gebeuren. Wat privacy en informatieveiligheid betreft, worden hieronder een aantal onderwerpen uitgelicht.

3.1 Geheimhoudingsplicht

Binnen de GGZ geldt er een wettelijk medische geheimhoudingsplicht. Een patiënt moet erop kunnen vertrouwen dat de informatie die hij/zij aan de hulpverlener verschaft niet zonder zijn/haar toestemming of zonder dat de wet dat toestaat voor andere doeleinden wordt gebruikt of aan anderen wordt verstrekt. De medische geheimhoudingsplicht verplicht de hulpverlener om te zwijgen over alles wat hem door de patiënt is toevertrouwd. Het gaat dus niet alleen om medische gegevens, maar ook om andere informatie die in de relatie tussen hulpverlener en de patiënt naar voren komt. De hulpverlener verstrekt daarom aan anderen dan de patiënt geen gegevens over de patiënt, tenzij de wet hier een uitzondering op maakt. Niet alleen de hulpverlener zelf is tot geheimhouding verplicht. Medewerkers die bij de zorgverlening betrokken zijn, maar niet vanwege hun eigen handelen een medisch beroepsgeheim hebben, hebben een van de hulpverlener afgeleid medisch beroepsgeheim. Dit geldt dan voor zover deze personen beroepsmatig op de hoogte raken van behandelgegevens van de patiënt. Dat kunnen bijvoorbeeld bestuurders, (dokters)assistenten, secretaresses, bewakingspersoneel, ICT-medewerkers of schoonmakers zijn.

3.2 Datalekken

Het kan voorkomen dat er in de omgang met persoonsgegevens wat verkeerd gaat. Wanneer er sprake is van een inbreuk op de beveiliging, waardoor persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, is er een datalek. Een datalek kan grote gevolgen hebben voor de privacy van de betrokkene(n). Voorbeelden van datalekken zijn een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand. In ernstige gevallen kan Fivoor de verplichting hebben om een datalek te melden aan de Autoriteit Persoonsgegevens. Het is daarom van belang dat alle datalekken intern worden gemeld door een VIM-melding te doen. De melding komt dan binnen bij je leidinggevende en een medewerker van Kwaliteit & Veiligheid, zodat er een zorgvuldige risico-inschatting gemaakt kan worden. Doe ook bij twijfel een VIM-melding.

3.3 Clean Desk Policy

Vanuit je medische geheimhoudingsplicht en overige privacywetgeving dien je zorgvuldig om te gaan met de persoonsgegevens van anderen. Binnen Fivoor wordt gevoelige informatie verwerkt, denk aan: informatie over iemands gezondheid, strafrechtelijk verleden en persoonlijk netwerk. Elke medewerker speelt een belangrijke rol in de bescherming van en de toegang tot persoonsgegevens en gevoelige informatie. Dit geldt zowel voor de toegang tot de informatiesystemen als voor de fysieke toegang tot werkruimtes of de toegang tot documenten. Binnen Fivoor wordt een Clean Desk Policy gehanteerd, wat inhoudt dat documenten netjes opgeruimd zijn, dat werkplekken vrij zijn van gevoelige persoonsgegevens en informatie en dat computers altijd vergrendeld worden bij het verlaten van de werkplek. De medewerking van alle medewerkers is van essentieel belang voor de privacybescherming en de informatieveiligheid.

3.4 Social Media

Social media kun je zowel privé als voor je werk gebruiken. Fivoor is ervan overtuigd dat social media een positieve rol kunnen spelen bij kennisverspreiding en kennisvergaring, het contact aangaan met de omgeving en het versterken van het imago van Fivoor. Daarom wordt het gebruik van social media van harte toegejuicht. Echter blijft het van belang zorgvuldig om te gaan met de informatie die je deelt via social media. Deel je gegevens over derden, vraag hier dan aan de betrokkenen expliciete toestemming

voor. Gebruik hiervoor een door Fivoor vastgesteld toestemmingsformulier. Wees je ervan bewust dat als je iets deelt op social media, dat mensen je ook in de rol van medewerker van Fivoor zien. Dus alles wat je plaatst kan in die context gelezen worden en effect hebben. Fivoor adviseert daarom om je social media zo in te stellen dat alleen jouw contacten de informatie die je deelt kunnen inzien. Ook de rol van behandelaar en patiënt moet duidelijk zijn. Daarom willigen medewerkers connectieverzoeken van patiënten via social media niet in. Woordvoering namens Fivoor wordt gedaan door de afdeling Communicatie en niet door individuele medewerkers. Tenslotte, als je zelf reageert op GGZ-gerelateerde berichten in de media, maak dan duidelijk vanuit welke rol je dit doet: professioneel of privé.

3.5 Rechten omtrent je eigen persoonsgegevens

Fivoor verwerkt ten behoeve van je indiensttreding en het uitbetalen van je salaris veel persoonsgegevens van de individuele medewerkers. Fivoor tracht hier zo zorgvuldig mogelijk mee om te gaan.

Omtrent je eigen persoonsgegevens heb je verschillende rechten:

- Het recht om een verzoek te doen tot inzage;
- Het recht om een verzoek te doen tot rectificatie;
- Het recht om een verzoek te doen tot verwijdering.

Deze verzoeken kunnen worden ingediend bij de afdeling HR.

3.6 Functionaris Gegevensbescherming

Binnen Fivoor is er een Functionaris Gegevensbescherming aangesteld. De Functionaris Gegevensbescherming houdt binnen de organisatie toezicht op naleving van de Algemene Verordening Gegevensbescherming (AVG) en werkt zelfstandig en onafhankelijk. Voor vragen over privacy en informatieveiligheid kun je je wenden tot de Functionaris Gegevensbescherming.