IPF
Innovatie Platform Fysiotherapie

INTRINSIEKE MOTIVATIE VOOR:

- INNOVATIE
- KWALITEIT
- FYSIOTHERAPIE

Annex II
Beveiligingsmaatregelen

Beveiligingsmaatregelen

#1 Informatie-, beveilighings-, en privacy-beleid	Er is een informatiebeveiligings- en privacybeleid opgesteld en geïmplementeerd om te voldoen aan de AVG, UAVG en eventuele richtsnoeren van de Autoriteit Persoonsgegevens. Dit beleid is intern gecommuniceerd.
#2 Governance	Er wordt periodiek een PDCA-cyclus uitgevoerd om beveiliging van persoonsgegevens (en van andere gevoelige informatie) te verbeteren.
#3 Personeel	Medewerkers die toegang hebben tot persoonsgegevens zijn gebonden aan geheimhouding. Medewerkers worden (mondeling en schriftelijk geïnformeerd over hun verantwoordelijkheden m.b.t. privacy en informatiebeveiliging. De organisatie ziet erop toe, dat medewerkers hun verantwoordelijke heden en verplichtingen hierover nakomen.
#4 Bedrijfsmiddelen	Apparatuur en software waarmee persoonsgegevens worden verwerkt worden toegewezen aan een eigenaar. De apparatuur en software wordt waar mogelijk versleuteld met een sterk wachtwoord en/of biometrische beveiliging. De apparatuur wordt niet onbeheerd achtergelaten.
#5 Toegangsbeveiligheid	De principes van ‘least privilege’ en ‘need-to-know’ worden toegepast op personeel en toegestane Subverwerkers. Er is beleid voor het tijdig intrekken of wijzigen van autorisaties bij verandering in de status van personeel, leveranciers, klanten, zakelijke partners, (sub)verwerkers of derden. Er wordt gebruik gemaakt van actuele en algemeen als veilig beschouwde vormen van versleuteling en encryptie ten behoeve van identificatie, authenticatie en autorisatie.
#6 Fysieke beveiliging	Er zijn passende maatregelen (zoals sloten, camera’s, alarmsystemen) genomen om de ruimtes waarin de Persoonsgegevens kunnen worden verwerkt, te beveiligen tegen onbevoegde toegang.

#7 Vulnerability / patch management	Er wordt periodiek beoordeeld of er kwetsbaarheden binnen de gebruikte applicaties, systemen en netwerken zijn. Patches en updates voor gevonden kwetsbaarheden worden doorgevoerd.
#8 Communicatiebeveiliging	Er zijn maatregelen getroffen om malware en misbruik van het netwerk en de systemen tegen te gaan en te detecteren (zoals firewalls en antivirussoftware van betrouwbare leveranciers).
#9 Contractmanagement (Sub)verwerkers	Met (Sub)verwerkers wordt een (Sub)verwerkersovereenkomst gesloten, die de (Sub)verwerker contractueel verplicht tot nakoming van gelijkwaardige verplichtingen in verband met de verwerking als in de verwerkersovereenkomst waar deze bijlage bij hoort.
#10 Beveiligingsincidenten	Er is een draaiboek waarin is omschreven hoe inbreuken in verband met persoonsgegevens worden gedetecteerd, geregistreerd en eventueel gemeld, in overeenstemming met de verplichtingen in deze verwerkersovereenkomst.