Datalekprotocol Brein en Welzijn (Laatste update: 09-01-2024)

1. Doel

Het doel van dit protocol is om een gestructureerde aanpak te bieden voor het detecteren, rapporteren, onderzoeken en reageren op datalekken binnen de psychologiepraktijk. Dit protocol is ontworpen om de vertrouwelijkheid, integriteit en beschikbaarheid van persoonlijke en gevoelige informatie te waarborgen.

2. Definities

Datalek: Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van, of de ongeoorloofde toegang tot persoonsgegevens.

3. Detectie van Datalekken

Datalekken kunnen worden gedetecteerd door verschillende middelen, waaronder:

- Monitoring van IT-systemen en netwerkactiviteit.
- Rapporten van medewerkers over verdachte activiteiten.
- Klachten van patiënten over ongeoorloofde openbaarmaking van hun informatie.
- Externe waarschuwingen over mogelijke inbreuken op gegevensbeveiliging.

4. Rapportageprocedure

a. Interne Rapportage: Alle medewerkers die op de hoogte zijn van een mogelijke datalek, zijn verplicht om dit onmiddellijk te melden aan de verantwoordelijke functionaris voor gegevensbescherming (FG) of aan een daartoe aangewezen persoon.

b. Registratie: Alle gemelde datalekken moeten worden gedocumenteerd, inclusief de aard van het lek, de getroffen gegevens, de mogelijke gevolgen en de acties die zijn ondernomen.

c. Externe Rapportage: Indien vereist door lokale wet- en regelgeving, moeten datalekken worden gemeld aan de relevante toezichthoudende autoriteit en/of aan de betrokken personen, zoals patiënten, binnen de vastgestelde termijnen.

5. Onderzoek en Beoordeling

a. Onderzoeksprocedure: Zodra een datalek is gemeld, wordt er een grondig onderzoek uitgevoerd om de oorzaak, omvang en impact van het lek vast te stellen.

b. Risicobeoordeling: Een risicobeoordeling wordt uitgevoerd om de potentiële gevolgen van het datalek voor individuen en de organisatie te bepalen.

6. Reactie en Mitigatie

a. Maatregelen ter beperking van verdere schade: Passende maatregelen worden genomen om verdere schade als gevolg van het datalek te beperken.

b. Communicatie: Betrokken personen worden op de hoogte gesteld van het datalek, inclusief de aard van het lek, de mogelijke gevolgen en eventuele maatregelen die zij kunnen nemen om zichzelf te beschermen.

7. Evaluatie en Preventie

a. Evaluatie: Na afloop van het incident wordt een evaluatie uitgevoerd om lessen te trekken en verbeteringen aan te brengen in het beveiligingsbeleid en de procedures.

b. Preventie: Maatregelen worden genomen om toekomstige datalekken te voorkomen, waaronder het verbeteren van de beveiliging van IT-systemen, het verstrekken van training aan medewerkers en het regelmatig evalueren van de naleving van het gegevensbeschermingsbeleid.

8. Training en Bewustwording

Alle medewerkers worden regelmatig getraind en geïnformeerd over het datalekprotocol en de procedures voor gegevensbescherming om het bewustzijn en de respons op datalekken te verbeteren.

9. Review en Bijwerking

Dit datalekprotocol wordt regelmatig geëvalueerd en bijgewerkt om ervoor te zorgen dat het blijft voldoen aan de geldende wet- en regelgeving en de beste praktijken op het gebied van gegevensbescherming.