**MODEL SPEERPUNTENBELEID**
**Privacybescherming & Informatieveiligheid (PB/IV) 2016**
Met dank aan Leo Kannerhuis, die dit stappenplan hanteert binnen de eigen organisatie

## 1. Inleiding

Vanwege de invoering van de wet meldplicht datalek per 1 januari 2016 worden in de loop van 2016 onderstaande procedures binnen <*naam instelling*> geactualiseerd en zo nodig opnieuw geïmplementeerd. Een en ander in afstemming met de branche-afspraken uit de werkgroep PB/IV GGZ van GGZ Nederland.

## 2. Procedures actualiseren en/of opstellen

- ***Privacyreglement***: afstemmen op model Privacy beleid ggz; Via ***privacyreglement*** patiënten en ouders/naasten/verwijzers informeren over *vernieuwde* privacy bescherming en informatieveiligheid;
- ***Procedure 'Melden datalek'*** binnen PDCA cyclus uitwerken en implementeren;
  - Opstellen ***'Melden datalek'***: wie doet wanneer wat?
  - Definitie verschil ***datalek en beveiligingsincident*** duidelijk hierin uitleggen;
  - Toelichten in een schema de ***verschillende TVB van alle functies***, van bestuurder tot sociotherapeut en huishoudelijk medewerker;
  - ***Meldprocedure automatiseren***: via e-mail, Incidenten meldformulier en/of Ticketsysteem ICT;
  - ***Registratieregister*** van datalek meldingen opstellen en bijhouden en opnemen in PDCA cyclus datalek meldingen;
- Toelichten in procedure: instellen ***Portefeuillehouder Gegevensbescherming (PG)*** (vooruitlopend op 'Functionaris gegevensbescherming').
- ***Autorisatie protocol*** voor toegang EPD en toegang mappenstructuur interne schijven actualiseren/opstellen; zie autorisatieprotocol model ggz: identificatie-authenticatieautorisatie;
- Overzicht maken/actualiseren van alle **registratie van privacygevoelige informatie** die moet worden doorgegeven aan de AP; zie meldformulier 'Registratie van privacy huishouding en gegevensverwerking' voor melding bij AP;
- Overzicht en ***classificatie*** van alle gegevensbewerkingen door en namens <naam instelling>; welke gegevens ver- en bewerken wij, hoe gevoelig zijn ze, wie mag ze op basis van die gevoeligheid lezen/bewerken, wie mag ze intern opvragen, wie mag ze extern opvragen et cetera;
- Procedure '***Bewerkersovereenkomst afsluiten***' opstellen/actualiseren en afstemmen op en integreren in de inkoopprocedure;

- Actualiseren ***inwerkschema's nieuwe medewerkers***: o.a. verplichte instructies/opleiding
    - voorafgaand aan ontvangst inlogcodes EPD en intranet; optie: opstellen ***e-learning module***
    - ***PB/IV-K&V*** die zowel bij indiensttreding als periodiek (elke 2 jaar bv.) moet worden gevolgd;
- Basisuitgangspunt: op alle niveaus in de organisatie bij alle processen: expliciet aandacht schenken aan bewustwording en ***permanente/automatische kans- en risicobeoordeling*** resulterend in een vooruitstrevende kwaliteit en veiligheidscultuur.
- ***Informatieveiligheidsbeleid*** op basis van NEN 7510 opstellen; ***Certificering*** volgens
    - ***NEN 7510*** starten als basis voor informatieveiligheid: technisch, organisatorisch en
    - 'menselijk'; checklist beschikbaar;
- Na certificering NEN 7510: aansluiten bij ***Z-CERT***?;
- Actualiseren ***Multimediabeleid***: wat mag je wanneer aan wie vertellen/delen en wat nooit;
- ***Sanctiebeleid*** ontwikkelen;
- ***Algemene verordening gegevensbescherming 2018***: nieuwe acties in beeld brengen en voorbereiden hierop.

### 3. Aanbevelingen werkgroep PBIV GGZ Nederland voor Awareness, houding en gedrag medewerker

Veiligheidscultuur en bewustwording van medewerkers activeren en afstemmen op PB/IV uitgangspunten o.a. door:

- Rapporteren over DLP registraties en de diverse meldingen van medewerkers als voorbeelden en daarbij opties noemen van veilige(r) alternatieven;
- Privacyproof werken stimuleren: acties bedenken;
- Instellen PB/IV commissie? Onderdeel K&V commissie? Doel: PG ondersteunen bij monitoren en stimuleren verantwoorde omgang met privacygevoelige gegevens en informatie
- Bewustwording datalek stimuleren.
- Maak een Personeelshandboek/**inwerkprogramma nieuw personeel** (leerprogramma bv verplichte e-learning (naar het voorbeeld van Tactus verslavingszorg).
- Maak een Communicatietrainingsplan.
- Speel in op de actualiteit, via een kort bericht/artikel, korte werkinstructie o.v.v. gegevens contactpersoon of een centraal emailadres.
- Maak FAQ > op intranet; via 'banners' op PC.
- Breng onder de aandacht via rollenspellen met elkaar of met acteurs; via 'mystery quests' (*bv er staat een 'politieagent' aan de receptie/ er hangt een 'buurvrouw' aan de telefoon die vraagt naar een bepaalde persoon; weet je wat je moet doen; is het beleid duidelijk?*).

- Bespreek PB/IV in korte casus + uitleg in een bestaand overleg of ander (digitaal) medium.
- Neem elke kans te baat om PB/IV onder de aandacht te brengen (kan op ernstige of op meer ludieke wijze bv via een quiz).
- Intervisie en ondersteuning in praktisch overzichtelijk stappenplan
- Invalprotocol ACM of andere toezichthouders opstellen en implementeren.
- Stel “ambassadeurs” aan: aandachtsfunctionarissen bij een afdeling/zorgeenheid op de
- werkvloer aanstellen; betrek deze bij de verschillende interne audits; laat deze rapporteren aan de Security Officer of FB.
- Stel PB/IV aan de orde via periodieke overleggen (werkoverleg, afd.- of teamoverleg, F&B-cyclus).
- Als sluitstuk: protocol wat gebeurt er (in gefaseerde stappen) als medewerkers niet veilig werken (incl. belonen).
- ***Gebruik DataLeakProtection:*** is een programma binnen ICT; detecteert privacylekken (zit in de Firewall); is zelf in te stellen via privacyinstellingen (*nadere informatie bij Dr. Leo Kannerhuis*);
- *Gebruik een* Meld-waarschuwingssysteem inrichten naast VIM (of geïntegreerd)+ bij een datalek moet direct een melding intern naar de FG gaan; zie ***PB/IV 3*** Model datalekken
- Stel bewerkersovereenkomsten op > gebruik modelbewerkersovereenkomst NVZ en pas evt. aan op uw praktijk.
- Neem de uitgangspunten in de contracten op in uw algemene (inkoop)voorwaarden