Overzicht van bijlagen
Implementatieprogramma Privacybescherming & Informatieveiligheid ggz (PB/IV)

PBIV 1 Beleidskader en Awareness, houding en gedrag medewerkers

- het Privacykader ggz met modelreglement,

Incl. uitleg van de zeggenschapsrechten van patiënt t.a.v. diens dossier

- Model Speerpuntenbeleid PB/IV 2016- 20..

Naar aanleiding van de werkgroepsessies in een overzicht gezet.

- Model Registratie privacyhuishouding en verwerkingen persoonsgegevens binnen de instelling (bijlage)

Toelichting: basis hiervoor vormt het Formulier melding AP: als u de eerste 7 vragen van dit webformulier beantwoordt, heeft u al de helft van je PBIV op orde; vraag 1 t/m 7 kun je per gegevenslevering vastleggen in privacybeleid; dit levert al een goede basis; vandaaruit kan er specifiek worden aangevuld.

- Model Verklaring van Toepasselijkheid voor de NEN 7510 (Tactus).

Toelichting: Bij het invullen van dit schema wordt duidelijk welke documenten nog ontbreken en welke acties dus nog op dat vlak moeten worden genomen.

- Model Classificatie en Risicoanalyse Gegevensverwerkingen

Toelichting:
Dit model kan de leden te helpen in hun wijze van classificeren en beschrijven van bedrijfsprocessen, informatiesystemen en informatie. Daarbij helpt het bij het uitvoeren van een (eerste) risicoanalyse op basis van een onderverdeling in beschikbaarheid, integriteit en vertrouwelijkheid van de te onderscheiden gegevens(verwerkingen). Bij deze richtlijn hoort het model “Management Systeem Informatiebeveiliging” (ISMS), als onderliggend beleidsdocument, ook als bijlage bijgevoegd

- Model “Management Systeem Informatiebeveiliging” (ISMS)

Toelichting:
Dit model hoort, als onderliggend beleidsdocument, bij het Model Classificatie en Risicoanalyse. Processen en activiteiten op het gebied van informatiebeveiliging worden met behulp van een procesbenadering doeltreffend samengebracht en beheerst.

- Competentieprofiel Functionaris voor de Gegevensbescherming (FG)

Relevante stukken op internet

- Richtsnoeren beveiliging persoonsgegevens van de AP.

PBIV 2 Registratie- Autorisatie-, authenticatie- en identificatiebeleid

- **Handreiking autorisatie EPD**

Deze handreiking maakt duidelijk aan welke eisen de autorisatie tot het elektronisch patiëntendossier (EPD) binnen de zorginstelling moet voldoen. Het is bedoeld als praktisch hulpmiddel waarmee GGZ Nederland haar leden wil ondersteunen.

Naast deze Handreiking wordt aanbevolen om diverse onderdelen van het EPD te classificeren. En voor toelichting op onderdelen van het EPD en definities van dossier of de patiënt/behandelgegevens, maak gebruik van:

- de Handreiking WGBO GGZ Nederland en
- de boekjes (m.n. deel 3) van de KNMG.

- **Referentiedomeinenmodel (RDG) GGZ**

Door NICTIZ is in samenwerking met GGZ Nederland en haar leden ontwikkeld. Het referentiedomeinenmodel GGZ (RDG) ondersteunt GGZ instellingen bij de inrichting van de informatievoorziening. Het RDG model kan o.m. dienen als basis voor de strategische koersbepaling voor ICT- ondersteuning, sourcingsbeslissingen of als kapstok voor de inrichting het applicatielandschap.

Het RDG bestaat uit een spreadsheet en een model. Ons advies is: pas het met gezond verstand toe en pas het aan uw specifieke doel aan. Herkenbaarheid, eenvoud en bruikbaarheid zijn de belangrijke uitgangspunten van het RDG. Acceptatie van het Referentiemodel is de belangrijkste succesfactor. Daarnaast is het goed onderhoud (zoals regelmatig evalueren en zonodig bijstellen) belangrijk.

- **Startkit identificatie en autorisatie**

Het kader en de benodigde stappen voor Identity Access Management (IAM)- vraagstukken zijn door experts van Surfnet en Platform voor Informatie Beveiliging (PvIB) geformuleerd en daarbij zijn aanpak- en oplossingsrichtingen uitgewerkt. Deze kennis is beschikbaar en kan op effectieve wijze door GGZ instellingen worden hergebruikt. Dit onderwerp is meer voor ICT-specialisten. Bijgevoegd een drietal documenten:

- korte toelichting op het onderwerp.
- Het Startkit Identity Management van Surfnet
- Autorisatiebeleid van PvIB.

Relevante stukken op internet

De Autoriteit Persoonsgegevens heeft de wettelijke regels uitgewerkt in de Richtsnoeren identificatie en verificatie van persoonsgegevens (kopie identiteitsbewijs).

PBIV 3 Modellen voor uitvoering in de praktijk

- Model Bewerkersovereenkomst

Naar het model van de NVZ, Nederlandse Vereniging van Ziekenhuizen, opgesteld, welke als uitgangspunt kan dienen voor de overeenkomsten met externe bewerkers. De standaard of het model NVZ is opgesteld door juristen en security officers van 13 ziekenhuizen en getoetst door een IT- en privacyrechtdeskundig advocaat. GGZ Nederland biedt deze haar leden onveranderd ter handreiking aan. Dit model met eisen en verantwoordelijkheden is in basis voldoende goed beschreven en inzetbaar maar zal per leverancier een nadere invulling moeten krijgen, o.a. het laten aansluiten op de hoofdovereenkomst.

- Model protocol patiëntendossier

Een model toe te passen door ggz-instellingen naar hun praktijk (e.e.a. naar aanleiding van onderzoek AP naar dossiervoering binnen instellingen en de Handreiking autorisaties EPD van GGZ Nederland

- Model patiënteninformatie verstrekken door receptie en secretariaat

Dit proces beschrijft de stappen van het secretariaat of andere ondersteunende medewerker wanneer men wordt geconfronteerd met een vraag over een patiënt.

- Model procedure binnenkomende externe post

Deze procedure omvat de poststromen die van buiten de instelling op de verschillende locaties van de instelling in ontvangst worden genomen. De procedure heeft ten doel de privacy van cliënten te beschermen en de poststromen en verantwoordelijkheden van de betrokken medewerkers te verhelderen.

- Model protocol Meldplicht Datalekken

Een praktische samenvatting over hoe te handelen bij beveiligingsincidenten en datalekken: wanneer moet men een datalek melden bij de AP en wanneer aan betrokkene(n)?

Voor een uitgebreide versie van beleid melding datalekken, zie Autoriteit Persoonsgegevens.

- Model Handleiding Receptie onaangekondigd bezoek toezichthouder

Een praktische instructie in drie stappen met een overzicht van contactpersonen en bijbehorende verantwoordelijkheden.

Relevante stukken op internet

Over NEN7510:

- http://www.ggz-connect.nl/bericht/3470/handreiking-informatiebeveiliging-in-control-over-informatiestromen; zie vooral checklist in link naar Word-document handreiking IB
- https://www.werkenmetnen7510.nl/normen
- http://www.norea.nl/index.aspx?FilterId=2423&ChapterId=12177&ContentId=74619