mevr. J. Berkelaar
(adres vertrouwelijk)

Stichting Benchmark GGZ
M. Erenstein, directeur
Rembrandtlaan 46
3723 BK Bilthoven

Datum : 20 februari 2017

Betreft : reactie op brief van B.J. Bos, kwaliteitsfunctionaris d.d. 15 februari 2017 inzake klacht verzamelen medische gegevens (ROM-gegevens) in SBG-databank

Geachte heer Erenstein,

De brief van de heer B.J. Bos, klachtenfunctionaris, d.d. 15 februari 2017, inzake bovenvermelde klacht, heb ik in goede orde ontvangen.

Wat betreft de gepseudonimiseerde gegevens in de SBG-databank, merk ik het volgende op.

U geeft in uw brief aan dat de gegevens in de SBG-databank zijn gepseudonimiseerd, dat de gegevens in de SBG-databank niet (meer) aan te merken zijn als persoonsgegevens en dat de Wet bescherming persoonsgegevens niet van toepassing is bij de ontvangst van de ROM-gegevens in de SBG-databank.

Onderstaande bevindingen bevestigen dat de gegevens in de SBG-databank wel degelijk zijn te kwalificeren als persoonsgegevens, namelijk:

1. Op basis van de erkenning van de artikel 29 werkgroep dat ook gepseudonimiseerde gegevens gekwalificeerd worden als persoonsgegevens in verband met onderkende mogelijkheden van herleidbaarheid.

2 Op basis van het onderzoek dat de Autoriteit Persoonsgegevens deed op 17 december 2015 naar de Diagnose Informatie Systeem-gegevens (DIS) bij de Nederlandse Zorgautoriteit, waarbij de Autoriteit vaststelde dat de data in het DIS door de Autoriteit worden beschouwd als persoonsgegevens. De DIS-databank is vergelijkbaar met de SBG-databank.

3. Door de koppeling van EPD en ROM-gegevens. Tevens is ook koppeling met DIS en Vektis mogelijk. Dit staat staat expliciet vermeld in de Benchmark Rapportage Module.
   Gegeven dat elke persoon een min of meer unieke behandelingshistorie heeft, wordt al snel helder dat het lastig te voorkomen is dat de data uit een gepseudonimiseerd record aan een patiënt te linken is.
   Voor zover ik heb kunnen nagaan, worden de volgende patiëntvariabelen opgeslagen en verwerkt in de databank van SBG: het versleutelde BSN, de viercijferige postcode, geboortejaar, leefsituatie, geslacht, etniciteit, opleidingsniveau, de vragenlijst die aan het begin en aan het eind van de behandeling door patient en/of de hulpverlener worden ingevuld, de zogenaamde ROM gegevens, DBC-gegevens zoals prestatiecode en gegevens over dwangmaatregelen in de GGZ (Argus-data).

Stichting Benchmark GGZ is geen onpartijdige organisatie die een betrouwbaarheid levert bij elektronische transacties omdat zorgverzekeraars de Stichting Benchmark GGZ financieren, drie bestuursleden van de Stichting Benchmark GGZ werkzaam zijn bij zorgverzekeraars en de zorgverzekeraars afnemers/gebruikers zijn van de Benchmark Rapportage Module. Stichting Benchmark kan om die reden niet worden aangemerkt als een Trusted Third Party (TTP).

In uw brief aan mij d.d. 15 februari geeft u aan dat de SBG-databank ISO-9001 gecertificeerd is. Dit betekent dat het managementinformatiesysteem is beveiligd, maar het betekent niet dat de SBG-

databank daarmee beschikt over een gecertificeerd informatiebeveiligingssysteem. In uw brief geeft u aan dat u de NEN volgt maar ik kan niet uit uw brief opmaken dat het informatiesysteem van de SBG-databank gecertificeerd is conform beveiligingsnormen voor informatiesystemen. Bovendien ben ik op uw website alleen een certificatie van het managementsysteem van DNV-GL ISO 9001 tegengekomen.

Op basis van het bovenvermelde, constateer ik dat:

1. de Wet bescherming persoonsgegevens van toepassing is op de SBG-databank,
2. de Wet op de geneeskundige behandelingsovereenkomst van toepassing is op de SBG-databank, aangezien er ook medische variabelen verwerkt worden,
3. er gegevens (ROM en Argus) aan de SBG-databank (derden) verstrekt zijn zonder dat de patiënt hier toestemming voor heeft gegeven (informed consent),
4. SBG de privacy van patiënten schendt en het medisch beroepsgeheim aantast,
5. SBG een wettelijke verplichting tot logging heeft,
6. de SBG-databank enkel ISO 9001 gecertificeerd is, wat slechts eisen bevat voor een kwaliteitsmanagementsysteem,
7. de SBG-databank, voor zover ik heb kunnen nagaan, geen enkele certificering heeft voor informatiebeveiliging, zoals:
   NEN 7510: informatiebeveilgiging
   NEN 7512: elektronische communicatie in de zorg
   NEN 7513: logging
   NEN 7521: toegang tot patiëntgegevens.

U stelt in uw brief aan mij d.d. 15 februari, dat er voor de SBG-databank geen wettelijke verplichting is voor certificering en u geeft aan dat de Wet bescherming van persoonsgegevens bij ontvangst van de ROM-gegevens niet van toepassing is.
Het bovenstaande in ogenschouw nemende, zou dit betekenen dat u zich mogelijk niet houdt aan de aan artikel 12 Wbp: verwerking in opdracht; geheimhoudingsplicht; artikel 13 Wbp: beveiliging; en artikel 14 Wbp: Beveiliging bij verwerking door een bewerker.

Gezien mijn bevindingen, vermoed ik dat er sprake is van onrechtmatige verwerking van (medische) persoonsgegevens in een database waarvan niet is vast te stellen of deze voldoende beveiligd is. Onduidelijk is of de wettelijk verplichte logging plaats vindt. Logging is van belang om vast te kunnen stellen of er onrechtmatige inzagen hebben plaatsgevonden en of er malware-aanvallen geweest zijn.

Ik verzoek u wederom dringend per direct het verzamelen en verwerken van de patiëntgegevens in de SBG-databank op te schorten vanwege het ontbreken van een informed consent, vanwege de mogelijke beveiligingsrisico's die er zijn bij de invoering en verwerking van uiterst privacygevoelige medische persoonsgegevens van ggz-patiënten, vanwege het feit dat het gaat om herleidbare persoonsgegevens en vanwege sterke vermoedens van onrechtmatige invoer en verwerking van patiëntgegevens in de SBG-databank.

Ik verneem graag spoedig uw schriftelijke reactie.

Met vriendelijke groet,

mevr. J. Berkelaar