



Datum: 15 februari 2017

Betreft: klacht verzamelen medische gegevens (ROM-gegevens) in databank van SBG

Geachte mevrouw Berkelaar,

Van mijn directeur ontving ik uw brief d.d. 12 februari 2017. Ik geef u graag in mijn hoedanigheid van kwaliteitsfunctionaris en geregistreerd Functionaris Gegevensbescherming van SBG bij de Autoriteit Persoonsgegevens een reactie.

Zorgaanbieder is Verantwoordelijke

Een behandelaar (dan wel de instelling waarbij hij/zij in dienst is, hierna: "Zorgaanbieder") is "Verantwoordelijke" voor de verwerking van persoonsgegevens van zijn patiënten. In beginsel mag de Zorgaanbieder met expliciete toestemming van de patiënt persoonsgegevens aan derden verstrekken. Er zijn echter ook andere wettelijke grondslagen die een gegevensverwerking kunnen legitimeren. Terecht merkt u in dat kader op dat de aanlevering van ROM-gegevens sinds 1 januari 2017 verplicht is gesteld in de ggz.

Het gaat echter de beantwoording van uw vragen te buiten om deze grondslagen in de onderhavige reactie te bespreken. Dit komt omdat SBG geen verantwoordelijke is in de zin van de Wet bescherming persoonsgegevens ("Wbp") als het gaat om de aanlevering en ontvangst van ROM-gegevens. Bovendien kwalificeren de bij SBG aangeleverde ROM-gegevens niet (meer) als persoonsgegevens in de Wbp. Ik licht dit kort toe.

De relatie tussen SBG en de Zorgaanbieder is momenteel juridisch zo ingericht dat de Zorgaanbieder altijd (de) verantwoordelijk(e) blijft voor de verwerking van persoonsgegevens van patiënten. Het is dan ook de Zorgaanbieder die zich (sinds 1 januari 2017 verplicht) dient aan te sluiten bij SBG en daarmee de opdracht geeft benchmark-informatie te ontwikkelen. Niet onbelangrijk is dat hier een heel technisch proces van meervoudige pseudonimisatie, encryptie en beveiligd (indirect) transport aan voorafgaat, voordat SBG überhaupt ROM-gegevens ontvangt en opneemt in haar database ten behoeve van de landelijke benchmark.

SBG ontvangt geen persoonsgegevens

De ROM-gegevens die SBG vervolgens ontvangt zijn echter niet direct dan wel indirect te herleiden tot patiënten. Daarmee kwalificeren de ontvangen ROM-gegevens – zoals hierboven aangegeven – niet als persoonsgegevens. Kort gezegd, wat SBG van uw zorgaanbieder ontvangt is niet terug te voeren op uw persoon. Het gevolg is dat de Wbp niet (meer) van toepassing is bij ontvangst van de ROM-gegevens in het domein (de database) van SBG. Dit is temeer wenselijk, omdat voor de ontwikkeling van de landelijke benchmark geen persoonsgegevens nodig zijn. Juist om dit proces juridisch te waarborgen zijn de *SBG Aansluitvoorwaarden Zorgaanbieders 1 oktober 2016* – ik neem gemakshalve aan dat u daarvan ook kennis heeft genomen – in het leven geroepen en (uniform) van kracht in het ggz-veld.

Uiteraard gaat SBG vanzelfsprekend zeer zorgvuldig om met alle ontvangen informatie (waaronder ROM-gegevens), omdat het gevoelige informatie blijft: de instellingsresultaten versus de landelijke benchmark betreft vertrouwelijke informatie voor de zorgaanbieder en zijn zorgverzekeraar(s).

Uw vragen

Gezien het voorgaande komt lijkt het mij raadzaam dat u uw bezwaren bespreekt met uw zorgaanbieder.



Uw Zorgaanbieder heeft waarschijnlijk een privacyreglement en een klachtenfunctionaris, waarmee u deze situatie kunt bespreken. Desalniettemin neemt SBG uw vragen uiterst serieus en zal ik deze beantwoorden.

Hieronder vermeld ik uw concrete vragen gevolgd door mijn antwoord.

“Ik verzoek u mij te berichten welke externe koppelingen er zijn met de SBG-databank.”

Tot op heden zijn er géén koppelingen tussen de SBG-database en andere databases. Het SBG-bestuur (waarin ook de het Landelijk Platform GGz zitting heeft) besluit op voorhand over de vraag of een toekomstige koppeling überhaupt gewenst is en (in overeenstemming met wet- en regelgeving) gemaakt mag worden. In het SBG Dataprotocol is dit uitdrukkelijk opgenomen. Ook rapporteren wij hierover op onze [website](#).

“Ik verzoek u mij te berichten of de SBG-databank gecertificeerd is conform NEN 7512 en NEN 7513.”

SBG is momenteel niet gecertificeerd conform de normen NEN 7512 en 7513. SBG is immers geen normadressaat van deze NEN-normen. Certificering is ook geen wettelijk verplichting voor SBG. Wel neemt SBG kennis van deze normen en hanteert deze algemeen geaccepteerde beveiligingsstandaarden als 'best practice' voor haar interne organisatie en haar uitgevoerde beleid. SBG is wél ISO 9001 gecertificeerd, waarbij controle op gecertificeerde leveranciers en het volgen van de NEN 7510 – voor zover het de (indirecte) uitwisseling van xml-bestanden betreft – onderdelen van audits zijn. De SBG-database wordt ook technisch onderhouden door een Nederlands bedrijf, met servers in Nederland, welk bedrijf ISO 9001, ISO 20.000 en ISO 27.001 is gecertificeerd.

Ik verzoek u mij te berichten of Stichting Benchmark GGZ in het bezit is van een sleutel om de pseudonimisering van de medische data ongedaan te maken.

SBG heeft geen sleutel om de (meervoudige) pseudonimisering ongedaan te maken. Dit proces is (technisch en organisatorisch) zo ingericht dat er geen mogelijkheid bestaat om dit ongedaan te kunnen maken. Meer hierover kunt u lezen op de [website](#) van Stichting ZorgTTP, welke Trusted Third Party hiervoor door uw Zorgaanbieder wordt gebruikt.

Tot slot verzoek ik u het verzamelen van ROM-gegevens per direct op te schorten om verdere schending van de privacy van cliënten/patiënten te voorkomen.

Vooropgesteld moet worden dat u uitsluitend rechten kunt uitoefenen ten aanzien van uw eigen persoonsgegevens. Daarnaast dient u zich in beginsel te wenden tot uw Zorgaanbieder, welke als Verantwoordelijke voor de verwerking van uw persoonsgegevens kan worden aangemerkt. Nu bovendien de door SBG ontvangen ROM-gegevens niet kunnen worden aangemerkt als persoonsgegevens, kan ik de door u gestelde schending van de privacy niet duiden.

Het is voorts niet aan SBG om het verzamelen van ROM-gegevens te beëindigen. SBG werkt op basis van een zogenaamd Bestuurlijk Akkoord tussen GGZ Nederland en Zorgverzekeraars Nederland, in opdracht van het genoemde SBG-bestuur. Vorig jaar verscheen het 'Model kwaliteitsstatuut ggz', opgesteld door GGZ NL, InEen, LPGGz, LVVP, NIP, NVvP, P3NL, Platform MEER GGZ, V&VN en ZN, waarin ROM en benchmark ook als veldnorm is gesteld. U refereert naar de verplichte aanlevering van ROM-gegevens, dus ik ga ervan uit dat u hiervan op de hoogte bent.



Graag benadruk ik het doel van SBG haar werk: kwaliteitsverbetering van de GGZ zorg voor patiënten. SBG onderschrijft dat GGZ-patiënten recht hebben op kwalitatief goede zorg en SBG ondersteunt dit door zorgaanbieders spiegelinformatie te bieden over behandelresultaten op populatieniveau.

Als u dat wenst geef ik graag een telefonische toelichting op deze brief. Ook bent u van harte welkom bij ons op kantoor – of elders – voor een nadere toelichting op bovenstaande antwoorden.

Tot slot, mijn dank voor uw aanmerking op de SBG Aansluitvoorwaarden Zorgverzekeraars. Ik heb deze aan het secretariaat gemeld en zij verwijderen '22', want bij dit punt hoort geen tekst.

Met vriendelijke groet,
Stichting Benchmark GGZ,

Bert Jan Bos,
Kwaliteitsfunctionaris / FG