Hoe een stoffig lijkend dossier opeens actueel wordt

In de Kamerbrief dd. 14 december van minister Tamara van Ark(VWS), staat op pagina 8 een passage over gedragscodes en de positie van de Autoriteit Persoonsgegevens(AP) daarbij. Het is volgens haar aan branches of sectoren in de zorg of deze een gedragscode aan de AP voorleggen voor het verwerken van (bijzondere) persoonsgegevens en wanneer. Daarnaast heeft de AP sinds het begin van de Algemene Verordening Gegevensbescherming(AVG) de bevoegdheid een gedragscode goed te keuren. Dit betekent dat er werkwijzen en processen in een gedragscode beschreven kunnen staan, **maar dat het wel afhangt van hoe de pet hangt bij de indieners ervan en/of van de AP of het tot een beoordeling c.q. goedkeuring komt.** Daardoor is het mogelijk dat zorgverzekeraars jarenlang werkten met een door de rechter afgekeurde gedragscode zorgverzekeraars en dat een nieuwe niet voorgelegd is aan de AP. En dat de AP geen oordeel velde/velt over een nieuwe.

Wat staat er?

Minister van Ark schrijft

“Daarnaast is door uw Kamer aangegeven dat er onduidelijkheid bestaat over de bevoegdheid van de Autoriteit Persoonsgegevens om gedragscodes goed te keuren voor de wijze waarop een branche of sector omgaat met persoonsgegevens. Artikel 40,vijfde lid van de Algemene Verordening Gegevensbescherming (AVG) geeft de Autoriteit Persoonsgegevens de bevoegdheid om gedragscodes goed te keuren. Een branche of sector die een gedragscode heeft opgesteld, kan aan de Autoriteit Persoonsgegevens vragen om deze goed te keuren.”

Taak AP, als ze het wil

Ze vervolgt:

“De Autoriteit gaat hiertoe over wanneer aan de eisen wordt voldaan. Het is hierbij vooral belangrijk dat de gedragscode een concrete uitwerking van de AVG biedt. In een dergelijke gedragscode worden de algemene normen uit de AVG immers concreter gemaakt. Deze zomer is voor het eerst een gedragscode goedgekeurd. Het gaat om de code van brancheverenigingNL digital. Het is aan de branche of sector een gedragscode voor te leggen en wanneer dat gebeurt. De Autoriteit Persoonsgegevens heeft immers al sinds de inwerkingtreding van de AVG de bevoegdheid een gedragscode goed te keuren.”

Slepende zaak

In een artikel op 11 december 2020 stipte ik al aan dat er sinds 2011 een procedure loopt van de Stichting KDVP richting de AP over het in strijd met wet en verdrag verwerken van medische persoonsgegevens door zorgverzekeraars. De verwerking legden de zorgverzekeraars vast in een Gedragscode zorgverzekeraars. Dit was omdat de in de Gedragscode Zorgverzekeraars beschreven procedures en bedrijfsprocessen in de ogen van de KDVP geen juiste uitwerking vormden van Wbp (Wet bescherming persoonsgegevens) en EVRM (Europees Verdrag voor de Rechten van de Mens). De zorgverzekeraars legden die gedragscode voor aan de toenmalige privacy-toezichthouder, het College Bescherming Persoonsgegevens(de voorganger van de AP).

Vervolg

De AP keurde de gedragscode in 2013 goed. De rechter in Amsterdam oordeelde op 13 november 2013 hierover. In die zaak tegen de AP, aangespannen door de KDVP, sprak de rechtbank uit dat het CBP bij de goedkeuring van de gedragscode op 13 december 2011 de in deze gedragscode vastgelegde

verwerkingsprocedures onvoldoende dan wel onjuist getoetst had aan vereisten voor de bescherming van privacy-rechten van patiënten/cliënten zoals vastgelegd in wet en verdrag. Enigszins verongelijkt trok na aandringen het CBP de goedkeuring van de gedragscode in. Nadien hebben de zorgverzekeraars geen herziene gedragscode voorgelegd aan het CBP of haar opvolger, de AP.

Dat is opmerkelijk te noemen omdat er sinds 2019 wel een nieuwe gedragscode van de zorgverzekeraars bestaat met betrekking tot verwerking van (bijzondere) Persoonsgegevens. Noch heeft de AP sinds 2019 enig signaal afgegeven dat zij eigenstandig die gedragscode onderzoekt.

Bizarre situatie

De minister verwoordt in haar brief aan de Tweede kamer een bizarre situatie. In een situatie waarin een eerdere versie van de gedragscode na rechterlijke tussenkomst uiteindelijk geen goedkeuring kreeg, blijkt dat de zorgverzekeraars de herziene versie zonder een goedkeurend oordeel van de privacy-toezichthouder gebruiken. Zulks in een constructie waarbij de makers van de gedragscode blijkbaar niet verplicht zijn die ter goedkeuring voor te leggen. En de AP niet verplicht is eigenstandig onderzoek te doen naar die nieuwe versie van de gedragscode. **Doordat beide partijen, gepardonneerd door VWS op de handen blijken te kunnen gaan zitten, gebeurt er niets** terwijl wel op basis van die gedragscode (bijzondere) persoonsgegevens verwerkt worden.

Wat een land, wat een land, waar dat allemaal maar kan! Wim Kan: uit het lied “twaalf miljoen oliebollen dansen in de pan.

W.J. Jongejan, 18 december 2020

Afbeelding van freestocks-photos via Pixabay

Roze olifant in AO VWS: toekomst zorgdata-uitwisseling zonder gespecificeerde toestemming

Op woensdag 9 oktober 2019 was het Algemeen Overleg(AO) van minister Bruins met de vaste Tweede Kamercommissie voor VWS. (Hier trouwens) alsnog te volgen. Het ging om de elektronische gegevensuitwisseling in de zorg en de gegevensbescherming. De reuzegrote roze olifant die tijdens het debat aanwezig was, betrof de toekomst van de uitwisseling van zorg-data zonder gespecificeerde toestemming. De Kamerleden bevroegen de minister indringend, maar niet op dat punt. Zij namen genoegen met de toezegging dat de minister in 2020 met een nieuw plan komt. Minister Bruins kondigde aan lid 2 van artikel 15 a in de Wet aanvullende bepalingen verwerking persoonsgegevens niet te doen ingaan. In dat lid zou die wet het gebruik van de gespecificeerde toestemming regelen. Hij doet het niet omdat hij het verwaterde model van gespecificeerde toestemming met 28 keuzemogelijkheden i.p.v. 160 bij nader inzicht toch niet geschikt vond voor invoering.

Opvraagbare zorgdata

Veel en indringend sprak men tijdens het AO over de noodzaak van een gemakkelijk elektronische overdracht van zorgdata. De Kamerleden spraken echter niet of nauwelijks over de basis waarop dit mogelijk is: de toestemming(opt-in) van de patiënt. Men moet bedenken dat bij gebruik van het Landelijk SchakelPunt(LSP) de voor toekomstig gebruik opvraagbaar gemaakte zorgdata alleen in te zien zijn als de betrokken patiënt toestemming heeft gegeven en er een behandelrelatie is. Een generieke toestemming ging velen veel te ver. Daarom bedacht Edith Schippers, voormalig minister van VWS, de gespecificeerde toestemming. De patiënt kon groepen van zorgverleners uitsluiten van inzage. De minister komt mede op basis van de conclusie van het Adviescommissie Toetsing Regeldruk(ATR) tot de conclusie dat de gekozen oplossing onwerkbaar is. Hij zegde in het AO toe in 2020 met een alternatief te komen dat recht deed aan de conclusies van de ATR.

Vertrouwen versus toestemming

Die concludeert om in de wet te opteren voor een stelsel waarin voor gegevensuitwisseling ten behoeve van goede zorg wordt uitgegaan van vertrouwen in de (zorg)instelling / professional en waarbij de uitoefening van de regierol via het inzagerecht loopt. In de conclusie van de ATR komt het woord toestemming nergens voor. De ATR lijkt een systeem voor te staan waarin de patiënt vertrouwt dat de zorgcommunicatie met de beste bedoelingen gebeurt met inzagerecht(=lees logging) achteraf.

Strijdig met AP

Wat de ATR in haar conclusie stelt is volkomen strijdig met het standpunt van de Autoriteit Persoonsgegevens(AP). De rechtsvoorganger van de AP was het College Bescherming

Persoonsgegevens(CBP). Bij de private doorstart van het LSP was het CBP zeer duidelijk over het bevragen van bij een zorgverlener opvraagbaar gemaakte zorgdata. Dat mocht alleen als er sprake is van een duidelijke toestemming van de patiënt: de opt-in-toestemming. Het CBP droeg VZVZ, als beheerder van het LSP, op de database van Nederlanders die onder de publieke periode van het LSP gevuld was met Nederlanders middels een opt-out-regeling te vernietigen bij de publieke start.(zie pg 6 en 7 in dit jaarverslag over 2012 van het CBP). VZVZ deed dat contrecoeur bij de aanvang van de publieke doorstart van het LSP.

Niet voorstelbaar

Het is niet goed voorstelbaar dat de AP plotseling vanwege de gebleken niet te implementeren gespecificeerde toestemming van koers zal veranderen en de noodzakelijkheid van een toestemming van de burger zal inslikken. Immers als we de gedachte van de ATR volgen, is er dan helemaal geen sprake meer van een opt-in- of opt-out-toestemmingsprincipe. In hun vertrouwensmodel zou iedereen in het systeem zitten met slechts controle achteraf.

Laten liggen

De Kamerleden hebben genoegen genomen met de toezegging van de minister dat hij in 2020 met een nieuw voorstel zal komen rond de opvraagbaarheid van medische data voor toekomstig gebruik. De zeer principiële discussie die daarbij gevoerd diende te worden is men uit de weg gegaan. Waarschijnlijk met de gedachte: dat zien we dan wel weer. Dat laat onverlet dat men als Kamerlid kritisch moet blijven als de minister een advies zegt te gaan volgen dat strijdig is met bepalingen en uitspraken van een toezichthouder. Voor mij was het de reuzegrote roze olifant in de Kamer die er wel was maar die niemand echt benoemde.

W.J. Jongejan, 12 oktober 2019

Het debat heb ik tijdens de uitzending van een live-blog voorzien. Op Twitter zoeken met AO en @ZorgICTZorgen levert zo'n 67 tweets op.

Afbeelding van Clker-Free-Vector-Images via Pixabay

Autoriteit Persoonsgegevens lekt URL van interne applicatie bij bekijken websites

Recent, 22 juli 2019, viel het mij voor de tweede maal in Google Analytics op, dat als iemand van de Autoriteit Persoonsgegevens(AP) deze website bezoekt de bron zichtbaar is. Ik bedoel dat Google Analytics de URL van het intranet van de AP toont. Nieuwgierig als ik ben hoe het bezoek aan de website ZorgICTZorgen zich ontwikkelt, kijk ik af en toe naar het real-time-overzicht. Op de kaart kan je met grote stippen zien in welke plaats iemand inlogt. Als iemand in Den Haag inlogt, ben ik altijd wat alerter. Meestal is de bron afgeschermd zodat die niet zichtbaar is. Van de AP dus blijkbaar niet. De reden van het bezoek aan mijn website door één of meerdere medewerkers van de AP was gelegen in een recente publicatie over de boete en last onder dwangsom die de organisatie oplegde aan het Haga-ziekenhuis. Het doet mij in ieder geval deugd te weten dat binnen de AP-organisatie men mijn blogs in ieder geval leest.

Niet eerste keer

Een jaar terug ongeveer viel mij hetzelfde al een keer op en deed ik melding ervan bij de AP middels het tip-formulier online. Ook gisteren deed ik een melding op deze wijze aan de AP. Beide keren kreeg ik geen enkele reactie hierop ondanks dat uitgebreide vermelding van NAW en contactgegevens. Ook al zou men het als ongevaarlijk en niet relevant beschouwen, lijkt me een retour-mail voor dit gratis advies niet overbodig. Ik voel me door het absoluut niet reageren gerechtigd nu hier vrij over te publiceren.

Afschermen

Van verreweg de meeste instellingen en bedrijven die mijn website bezoeken is de bron-URL niet te zien. Een enkele keer wel. Zo zag ik ook enkele dagen terug de URL van het Ikazia-ziekenhuis passeren.(www.ikazia.nl). De bedrijven die nooit moeite doen om aanwezigheid geheim te houden zijn de webcrawlers. Een webcrawler of spider is een bot die het internet op een methodische en geautomatiseerde manier doorbladert. Spiders maken veelal een lokale kopie van de gevonden pagina’s om deze later te kunnen verwerken en indexeren voor bijvoorbeeld zoekmachines.

Keuze

Op mijn website staat in de privacyverklaring expliciet vermeld dat de website gebruik maakt van een cookie van Google Analytics. Daarbij staat ten overvloede vermeld dat men door het veranderen van instellingen in de webbrowser de cookie kan weigeren.

URL

De zichtbare URL van de AP is: **Intranet.CBP.local.** Je kunt in de vermelding op de schermafbeelding die ik maakte meteen zien dat men na de naamswijziging op 1 januari 2016 niet de

moeite heeft genomen om de naamgeving van een intern systeem aan te passen. Voor die datum heette de toezichthouder College Bescherming Persoonsgegevens(CBP). Naast naamborden, websites en briefpapier had het in de lijn van de lijn van verwachting gelegen om ook de naamgeving van het intranet aan te passen.

Onverstandig

Men de lekt URL van een interne applicatie en dat is informatie die van nut kan zijn bij social-engineering. Bijvoorbeeld de AP een HTML-mail sturen met een klikbare link die zogenaamd een bij de gebruiker herkenbare/vertrouwde URL opent, maar in werkelijkheid een website laadt met, zeg, 1) een nep-inlogscherm om credentials te stelen, en/of 2) een JavaScript-gebaseerde poortscanner om het interne netwerk in kaart te brengen, en/of 3) met een heel ander scenario: om zich voor te doen als IT-medewerker o.i.d. De blootstelling van de informatie is natuurlijk wel beperkt tot websites die op de intranet-site worden aangeklikt. Maar dan wel óók tot servers van eventuele derde partijen waarvan de website content laadt – zoals vele servers van online advertentiebrokers.

Advies

Het lijkt me verstandig dat een toezichthouder geen sporen achterlaat als haar personeel op het internet websites bekijkt. Als het mijn website betreft kan het net zo goed gebeuren bij websites met minder degelijke inhoud, zoals gok- en porno-sites. Niets menselijks zal een medewerker van de AP vreemd zijn. Dus moeten systeembeheerders waken voor het achterlaten van bezichtigingssporen door personeel van de AP. Sporen die het binnendringen in een systeem vergemakkelijken.
 De applicatie Google Analytics is overigens een nuttig en wereldwijd gratis te verkrijgen programma en veel gebruikt programma en geenszins een manier om de AP doelbewust te volgen.

W.J. Jongejan, 24 juli 2019

Afbeelding van Clker-Free-Vector-Images via Pixabay

Makkelijk scoren voor verder lakse Autoriteit Persoonsgegevens bij Haga-ziekenhuis

Op 16 juli 2019 maakte de Autoriteit Persoonsgegevens(AP) bekend dat ze Het Haga-ziekenhuis in Den Haag een zeer hoge boete van 460.000 euro en een forse last onder dwangsom oplegde. Het besluit dateert van 18 juni 2019. Het gaat om de nasleep van een berucht datalek uit april 2018. Toen raakte bekend dat 85 ziekenhuismedewerkers onterecht het medische dossier van de "reality ster Barbie" ingezien hadden. Het kwam naar buiten door een tip via de klokkenluiderssite PubLeaks aan de tv-rubriek EenVandaag. Ik schreef er in 2018 drie keer over. (A, B, C). De AP kwam toen in actie en deed onderzoek bij het Haga-ziekenhuis. Eigenlijk kon de AP het zich niet permitteren om geen onderzoek te doen en geen maatregelen af te kondigen vanwege de forse publiciteit rond deze gebeurtenis. Bij de AP lopen meerdere zaken waarbij sprake is van schending van de privacyrechten van burger in de zorg waar de AP geen beslissing neemt en/of onderzoek op de lange baan schuift.

Geen 85 maar 100

De AP publiceerde heden een onderzoeksrapport uit maart 2019 en een boetebesluit van 18 juni 2019. In dat laatste is te lezen(blz. 4/25) dat van de 197 personen die inzage hadden in dossier van “Barbie” honderd personen dat onrechtmatig deden. In april 2018 had het ziekenhuis nog gemeld dat het om 85 personen ging, die niets met de behandeling te maken hadden, Het gaat dus om een beduidend groter aantal onrechtmatige daden dan waarvan de AP in het onderzoeksrapport zelf ook nog melding maakt. Geen van de mensen die onrechtmatig inzage hadden is trouwens ontslagen. Ze werden “berispt”.

Toegangscontrole

Uit het rapport blijkt dat het mogelijk was op drie manieren toegang te krijgen tot een dossier. Met twee-factor-authenticatie(personeelspas plus wachtwoord/inlogcode), met één-factor-authenticatie(wachtwoord/inlogcode) en een noodknop-procedure. Dat laatste is een toegang in noodsituaties, waarbij het personeelslid toegang krijgt maar wel op een scherm moet noteren waarvoor die toegang noodzakelijk was. De één-factor-authenticatie beschouwt de AP als verregaand onvoldoende en mag van haar niet blijven bestaan naast de twee-factor-authenticatie. Daarnaast controleerde het ziekenhuis de logging (het vastleggen van de inzage) op een zeer insufficiënte wijze. Van één patiënt per twee maanden, dus zes per jaar controleert men de log-gegevens, op een totaal van een paar honderdduizend patiëntdossiers per jaar!! Verregaand insufficiënt noemt de AP dat terecht. In de verste verte lijkt dat op een afdoende, intelligente, consequente controle.

Eerdere melding bij AP

Het is zeker niet de eerste keer dat de AP op de hoogte is gesteld van onterechte inzagen in medische dossiers. Mij is

een geval bekend(van vijf jaar terug) van een ex-GGZ-patiënt die aangifte bij de AP en bij de Inspectie Gezondheidszorg en Jeugd(IGJ) deed van het vele malen onterecht inzien van het dossier door nogal wat onbevoegden. De rechtsvoorganger van de AP, het College Bescherming Persoonsgegevens(CBP), liet toen weten er een notitie van gemaakt te hebben, maar deed er vervolgens niets mee. Men had toen nog niet de mogelijkheid om hoge boetes, zoals nu op te leggen. Wel kon het CBP toen beperkte boetes opleggen bij het verzaken van de meldplicht van datalekken en een last onder dwangsom of bestuursdwang toepassen. De patiënt meldde het zelf, waardoor gerust gesteld kan worden dat de instelling verzuimd had het datalek te melden. De IGJ draaide zich eruit door te verwijzen naar het “grondige” onderzoek van het instellingsbestuur.

Lastige beslissingen

In diverse zaken neemt de AP geen ferm standpunt in, traineert beslissingen en poogt ze zelfs als er rechtszaken komen die eindeloos te vertragen en soms met beroep op geheimhouding te beïnvloeden. Ik doel daarbij op zaken rond het DBC Informatie Systeem(DIS) en Routine Outcome Monitoring(ROM)-data. Daar spelen hele grote belangen een rol waardoor de AP op eieren loopt om maar geen beslissing te hoeven nemen.

Zieligheidscriterium

In de casus met de boete voor het Haga-ziekenhuis is het zieligheidscriterium al van stal gehaald door het ziekenhuis. Het Ziekenhuis heeft ter zienswijze-zitting een beroep gedaan op beperkte draagkracht, onderbouwd met de concept jaarrekening 2018(blz. 23/25 boetebesluit). In dat kader voert zij aan dat het Haga-ziekenhuis in 2018 een uitsluitend als “vertrouwelijk” genoemd bedrag heeft overgehouden ten gevolge van incidentele baten. De AP ziet hierin echter geen aanleiding om aan te nemen dat het ziekenhuis gezien haar financiële positie een boete van € 460.000,– niet zou kunnen

dragen.

Makkelijk scoren

Uit het voorgaande moge blijken dat de AP bij dit ziekenhuis makkelijk scoren had. En zo daadkracht kon tonen die haar andermaal nogal eens ontbeert. Bovendien was de optie om niets te doen ook geen begaanbare weg. Het zal er waarschijnlijk op neer gaan komen dat het ziekenhuis gaat procederen tegen de boete van de toezichthouder. Zaken bij een andere toezichthouder, de Autoriteit Consument en Markt, hebben laten zien dat een dergelijke rechtsgang gunstig is voor de instelling.

W.J. Jongejan, 17 juli 2019

Rupsje Nooitgenoeg NZa gaat onder druk een blaadje minder eten

Niet zo prominent was in de nieuwsbrief van de Nederlandse Zorgautoriteit(NZa) op 23 november 2018 te zien dat binnenkort een zeer belangrijke verandering doorgevoerd wordt. De NZa maakte kenbaar dat per 15 april 2019 een wijziging plaats vindt in de inhoud van de Minimale DataSet(MDS) die

zorggaanbieders in de specialistische geestelijke gezondheidszorg(GGZ) moeten aanleveren aan het DIS. Dat staat voor het Diagnose Behandel Combinatie(DBC) Informatie Systeem. Daarin slaat de NZa op persoonsniveau gegevens op over medische diagnoses en de behandeling. Ze stelt nu dat na 15 april het aanleveren van de hoofddiagnose volstaat. De informatie over diepere niveaus vraagt men dan niet meer op. Tegelijk meldt de NZa dat informatie over die diepere niveaus die de afgelopen jaren aangeleverd is niet meer voor verdere verwerking beschikbaar zal zijn. **Let wel: hier schrijft de NZA niet dat die dat vernietigd worden, maar dat ze niet meer beschikbaar zijn.** Het is een zeer beperkte aanpassing . Maar deze stap moet wel gezet zijn onder druk van een rechtszaak. Die betreft een eerdere weigering van de Autoriteit Persoonsgegevens om handhavend op te treden tegen de NZa inzake aanlevering van (zeer gedetailleerde) behandelinformatie op persoonsniveau bij het DIS.

Rupsje nooitgenoeg

De NZa geeft met het DIS blijk van een enorme datahonger en is een echt Rupsje Nooitgenoeg. Het zijn data die verzameld worden om beleid te ontwikkelen en ondersteunen in de zorg. Het trieste is dat er bewust voor gekozen is om op persoonsniveau centraal persoonsgegevens te verzamelen. Ook al zijn die gegevens (dubbel) gepseudonimiseerd, het blijven persoonsgegevens. Dat inzicht is de laatste paar jaar steeds duidelijker uitgekristalliseerd en vormt de basis voor verzet tegen het DIS en de ROM-data-verzameling. Voor beleidsontwikkeling en ondersteuning is het totaal onnodig om op persoonsniveau centraal data te verzamelen. Het College Bescherming Persoonsgegevens, de rechtsvoorganger van de Autoriteit Persoonsgegevens, stelde in 2006 al dat een dergelijke dataverzameling tot de zeer risicovolle activiteiten behoort. De hoeveelheid data die de NZa verzameld, vooral in de MDS van de specialistische GGZ is schrikbarend groot. Onder dit artikel heb ik de hele set die

de NZa na 15 april 2019 nog wil hebben tegen mijn gewoonte in om een artikel beperkt te houden toch eens afgedrukt. U krijgt dan ook een indruk van de enorme administratieve last die het aanleveren van deze data met zich meebrengt.

Beperking

Wat is nu die beperking die de NZa doorvoert. Binnen de MDS diende de volledige DSM-IV diagnose gespecificeerd te worden. Daarbij gaat het om een psychiatrische diagnose die verpakt is in 5 assen: primaire symptomatologie (de 'psychische ziekte'), achterliggende persoonlijkheidsstoornissen, (bijkomende) somatische ziekten, psychosociale en uitlokkend factoren en het niveau van functioneren(geschat op een schaal van 1 tot 100). Het behoeft geen betoog dat zoiets een enorm gedetailleerde informatie is over een persoon. Vanaf 15 april 2019 dient alleen de hoofddiagnose, maar niet die van de andere assen aangeleverd te worden.

Rechtszaak

In 2017 diende voor de Rechtbank Midden Nederland de zaak AWB-16_4199 die de burgerrechtenvereniging Vrijbit tegen de Autoriteit Persoonsgegevens(AP) had aangespannen. Als derde partij heeft de NZa ook aan de zitting deelgenomen. De reden was de eis tot handhaving door de AP tegen het verstrekken en verwerken van gegevens door de NZa via het DIS. De meervoudige kamer van de rechtbank deed een tussenuitspraak waarin de AP en NZa de gelegenheid werd geboden om alsnog te voorzien in maatregelen waarmee de gevolgen van de onrechtmatige verwerking van medische persoonsgegevens door het DIS zonder toestemming van de patiënt teniet zouden worden gedaan. De rechtbank deed de uitspraak onder voorzitterschap van mr. Verburg die zich tijdens de zitting uiterst kritisch tegen de AP en de NZa toonde.

Traineren

Uit welingelichte bron vernam ik dat zowel de AP als de NZa er

alles aan hebben gedaan om de mediatie te traineren en geen veranderingen in hun handelen aan te brengen. Over de voorzitter van de rechtbank, mr. Verburg, werd in de loop van 2017 bekend dat die benoemd zou worden bij de Raad van State. Het is zeer waarschijnlijk dat het traineren daar deels mee te maken had, omdat men na zijn overstap op een minder kritische rechter hoopt. Daarnaast is het zo dat het handelen van de AP in meer zaken zich kenmerkt door het traineren van beslissingen. Zo wacht een handhavingsverzoek over het door de Stichting Benchmark GGZ verzamelen van ROM-data **al 89 weken** op een beslissing van de AP. De burgerrechtenvereniging is inmiddels het traineren zat. Het gaat voor Vrijbit nu al om 17 maanden na de uitspraak van de rechtbank midden juli 2017. Een nieuwe zitting staat voor februari 2019 op de rol bij de rechtbank.

Eerder vertoond

Al eerder is vertoond dat een data-verzamelende instelling vlak voor een rechtszitting een aanpassing doet aangaande de gewraakte materie. Zo veranderde de Stichting Benchmark GGZ(SBG) enkele weken voor een rechtszaak van twee patiënten op 13 juli 2017 tegen SBG over ROM-data de wijze waarop een aantal cruciale data aangeleverd dienden te worden. Ook kwam twee dagen voor die rechtszaak de mededeling dat SBG begin 2019 op zou houden te bestaan en op zou gaan in een nieuw op te richten kwaliteitsinstituut voor de GGZ, thans Akwa genaamd. Het is een beproefde tactiek om de beslissing van de rechter te beïnvloeden.

De huidige aanpassing door de NZa past in zo’n rijtje, maar is beslist onvoldoende. Het hele systeem van het DIS waarin op persoonsniveau centraal zorgdata worden verzameld is onnodig voor het doel: beleidsontwikkeling en -ondersteuning in de zorg. Dat kan even goed op basis van geaggregeerde data verkregen met geautomatiseerde rapportages gemaakt op basis van gegevens die (decentraal) bij zorgverleners aanwezig zijn.

W.J. Jongejan, 11 december 2018

12 december: enkele kleine tekstuele aanpasssingen gemaakt in alinea Rechtszaak

_____

Minimale dataset vanaf 15 april 2019:

Identificatie zorgaanbieder

Unieke identificatie zorgaanbieder (AGB-code) 1

Patiëntgegevens (gepseudonimiseerd):

-naam cliënt

-geboortedatum

-geslacht

-postcode

-Burgerservicenummer

-unieke identificatie zorgverzekeraar (conform UZOVI-register)

-eerste inschrijfdatum

-laatste uitschrijfdatum

Hoofdbehandelaar

- AGB-code (op persoonsniveau) en diens beroep

Verwijzer

– Het type verwijzer:

1. verwezen patiënt vanuit de eerste lijn (o.a. huisarts, bedrijfsarts)
2. verwezen patiënt vanuit een (andere) ggz-instelling, instelling voor medisch specialistische zorg of ggz-praktijk
3. verwezen patiënt vanuit de crisis zorg of seh.
4. eigen patiënt
5. verwezen patiënt, maar verwijzer heeft geen AGB-code (bijvoorbeeld in geval van een verwijzing naar de crisis zorg, buitenlandse zorgaanbieder, bureau Jeugdzorg)
6. zelfverwijzer
7. bemoeizorg

- AGB-code verwijzer (op persoonsniveau), indien er sprake is van type verwijzer genoemd onder 1 tot en met 4

Productie per cliënt

1. Dbc-trajecten

Dbc:

-zorgtrajectnummer

-begindatum zorgtraject

-einddatum zorgtraject

-circuit

-zorgtype

-DSM diagnoseprofiel op hoofdgroepniveau1

– aantal minuten directe en indirecte patiëntgebonden tijd van iedere hoofdbehandelaar en iedere medebehandelaar en diens beroep

-totaal bestede directe en indirecte patiëntgebonden tijd per dbc

-afspraaknummer/code

Behandeling:

-begindatum dbc-traject

-einddatum dbc-traject

-afsluitreden dbc

-Gedeclareerde prijs

-declaratiedatum

Geleverd zorgprofiel binnen het dbc-traject:

-activiteiten, verrichtingen, overige deelprestaties en producten, zoals gedefinieerd in de Nadere regel gespecialiseerde ggz

-datum + tijdsduur activiteiten/producten

-beroep behandelaar

-deelfactor groepscontacten

Aan structureel onrechtmatige aanmeldingen in LSP moet eind komen

Onlangs kreeg ik zicht op hoe een apotheek op volkomen illegale wijze, volgens de marketingtruc 'ja tenzij' mensen aanmeldt alsof zij toestemming verleend zouden hebben om hun medische gegevens via het Landelijk Schakel Punt(LSP) te laten uitwisselen. De apotheek stopte dit voorjaar hiertoe een brief in de zakjes waarin afgehaalde medicijnen werden meegegeven. Daarin stond aangekondigd dat als men niet voor een bepaalde datum bezwaar aantekende, er na 14 juni 2017 voor hen het LSP zou worden aangezet onder vermelding dat zij door niet te reageren toestemming daarvoor zouden hebben gegeven. Daarnaast werden mensen ook nog eens op onrechtmatige wijze onder druk gezet dat toestemming geven in het belang van hun gezondheid is omdat er zonder aansluiting bij het LSP bijvoorbeeld in de avonduren via een dienstapotheek geen goede medicatie gegeven zou kunnen worden. Heel vilein suggereert het briefje bovendien dat men alleen maar geen toestemming bij de apotheek zou hebben staan, omdat men de klant al een poos niet aan de balie had gezien vanwege de bezorging van de medicijnen. De apotheek heeft met het sturen van deze brief en het aanmelden van mensen zich onmiskenbaar schuldig gemaakt aan het onder druk zetten van patiënten zodat zij niet in vrijheid zelf kunnen beslissen en aan het gebruik van een wettelijk verboden opt-out-constructie.

Van Gogh-apotheek

De boosdoener is de van Gogh-apotheek in Haarlem. Door op de beschreven wijze medische gegevens van hun klanten open te zetten voor landelijke opvraging door zorgverleners waar betrokkenen geen enkele relatie mee hebben, is bovendien sprake van een grootschalig datalek van uiterst gevoelige

medische persoonsgegevens. Omdat VZVZ(beheerder van het LSP) geen uniforme procedure hanteert voor het verkrijgen, registreren en loggen van aangemelde toestemmingen, valt te vrezen dat deze apotheek niet de enige is. Uit onderzoek van Burgerrechtenvereniging Vrijbit, blijkt hoe apotheken, het al dan niet daadwerkelijk verleende toestemmingen verzamelen, organiseren via regionale samenwerkingsverbanden. Volgens de Wet bescherming persoonsgegevens(Wbp) mogen mensen enkel worden aangemeld als zij daarvoor in vrijheid zonder uitoefening van druk en op grond van correcte en heldere informatie ondubbelzinnig toestemming voor hebben verleend.

Bij de doorstart van het LSP is door de voorganger van de huidige Autoriteit Persoonsgegevens(het CBP) op vragen van Nictiz (die het toenmalig door de Eerste Kamer verboden Landelijk Elektronisch PatiëntenDossier(L-EPD)-systeem) over deed aan de private partij VZVZ) duidelijk gesteld dat er sprake moest zijn van de expliciete toestemming van de patiënt via een opt-in systeem.

Geschiedenis

In 2008 had de toenmalige minister van VWS, Ab Klink, bepaald, dat de medische gegevens van iedere burger verplicht beschikbaar werden gesteld voor elektronische uitwisseling via het LSP. Pas toen er grote maatschappelijke onrust ontstond, werd er een uiterst gecompliceerde mogelijkheid aangekondigd waarbij mensen alsnog bezwaar zouden kunnen gaan maken tegen de uitwisseling van hun medische data via het Landelijk Elektronisch PatiëntenDossier(L-EPD). Toen na deze valse start van het L-EPD de Eerste Kamer de hele publieke L-EPD-invoering blokkeerde, werd het concept niet losgelaten, maar zodanig gewijzigd dat er een zogenaamde ‘private doorstart’ werd gemaakt. Daarbij kwam de verantwoordelijkheid niet langer in handen van de overheidsdienst Nictiz, maar in handen van een private partij. Deze Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ), kreeg het oorspronkelijke systeem onder haar hoede met dien verstande dat de bestaande database

gevuld met opt-out-toestemmingen opgeschoond diende te worden.

Acht miljoen mensen werden zo uit de LSP-index verwijderd en alle bezwaren van mensen die aangegeven hadden dat ze niet accepteerde dat hun gegevens via het EPD beschikbaar kwamen werden ongeldig verklaard.(waardoor tot op de dag van vandaag er nog steeds mensen zijn die stellig van mening zijn dat zij expliciet tegen het huidige systeem hebben geprotesteerd omdat zij in 2008, 2009 bezwaar aantekenden).

Opt-in

Cruciaal voor de private doorstart werd geacht dat het geen opt-out (ja tenzij) maar opt-in systeem zou worden. Daarmee werd gesuggereerd dat mensen enkel in het systeem zouden komen als zijzelf daar expliciet toestemming voor gaven. Door deze verschuiving werden en passant alle bezwaren tegen het systeem qua onveilige dataverwerking, het gebruik van het BSN door een partij die daar niet over mag beschikken, en onwettige constructies met betrekking tot de verantwoordelijkheid bij misbruik van medische gegevens en gevraagde generieke toestemming voor onvoorziene toepassingen, ter zijde geschoven. Feit is dat in 2014 het CBP, na een uiterst beperkt onderzoek(steekproef van 149 personen), al onrechtmatig genoteerde toestemmingen constateerde. Dat werd toen als onbelangrijk incident afgedaan omdat het niet zou gaan om mensen die geen toestemming hadden gegeven maar slechts om administratief niet correct vastgelegde toestemmingen.

Werkwijze apotheek

De brief van de van Gogh-apotheek in Haarlem is gedateerd op 22-05-2017 met als bezwaar-deadline 24-06-2017. De folder van VZVZ die hierbij werd meegestuurd lijkt een poging om de illegale toestemmingsvraag een correct tintje te geven. Maar zelfs die voorlichtingsfolder geeft geen correcte informatie. Deze werkwijze, om via een stilzwijgende opt-out procedure

toestemming te veronderstellen en vervolgens te registreren en door te geven aan het LSP voor opname in de verwijsindex, is niet alleen een onrechtmatige handelswijze van de betrokken apotheker, maar maakt ook dat alle aanmeldingen van toestemming vanuit deze apotheek vanaf 14-6-2017 niet langer als rechtmatig kunnen worden beschouwd en uit de verwijsindex verwijderd dienen te worden. Daarnaast is het maar helemaal de vraag of de vreemde opt-out-constructie enkel de mensen treft die de brief bij hun medicijnen meekregen of ook voor alle andere patiënten die bij deze apotheek hun medicatie krijgen, of ook voor de familieleden van de mensen die een dergelijke brief meekregen, maar toevallig geen medicijngebruikers zijn. Vandaar dat alle klanten van deze apotheek geïnformeerd dienen te worden over de onjuiste registratie van 'toestemming' alsook over het opvragen van medische gegevens zoals dat heeft plaatsgevonden op basis van de ten onrechte geregistreerde toestemmingen.

Vrijbit

Burgerrechtenvereniging Vrijbit heeft aan de toezichthouder bescherming persoonsgegevens een formeel handhavingsverzoek gestuurd om hiervoor zorg te dragen. Bovenstaande gang van zaken is één van de methodieken waardoor op illegale wijze toestemmingen vergaard worden door zorgaanbieders. Het gaat met name ook op het landelijk op grote schaal voorkomen van onrechtmatige aanmeldingen door met name de apothekers. Ook hierop ziet het handhavingsverzoek evenals het eerdere handhavingsverzoek wat gebaseerd was op de praktijkvoorbeelden van individuele gevallen waarin mensen ontdekten ten onrechte te staan aangemeld.

VZVZ

VZVZ poogt zich er altijd uit te draaien door te stellen dat zij de toestemmingsvereisten voldoende duidelijk uitleggen in hun folders en voorlichtingsbijeenkomsten. Maar omdat VZVZ een systeem beheert dat onrechtmatig- dan wel helemaal niet

verkregen- toestemmingen als grondslag voor aanmeldingen faciliteert, zijn zij uiteraard wel degelijk aansprakelijk. Dit geldt zowel voor het runnen van een systeem waarbij mensen er niet van op aan kunnen dat hun medische gegevens niet ter beschikking worden gesteld aan partijen waar zij geen toestemming voor gaven, als voor de manier waarop de controle hierop systematisch onmogelijk wordt gemaakt. VZVZ voelt wel nattigheid, want in de nieuwsbrief van juli 2017 is een apart stukje aan dit onderwerp besteed. Daarin refereert men aan de recente belangstelling voor verkregen toestemmingen naar aanleiding van de voorbeelden van mensen die onterecht in het systeem bleken te 'zitten' en berichtgeving van het tv programma Radar waaruit blijkt dat een substantieel deel van de bevolking geen idee heeft of zij staan aangemeld(en dus wie er over hun medische gegevens kunnen beschikken). Het VZVZ-toestemmingsformulier is inmiddels na jaren zodanig aangepast dat daarop nu wel wordt vermeld dat het over het LSP gaat, maar de informatie blijft te sturend om in vrijheid gegevenstoestemming mogelijk te maken.

Marketing-truc

Aan het op illegale wijze vullen van de LSP-index met vermeende toestemmingen moet een einde komen. Daarbij moet de AP niet schuwen om overtreders aan te pakken voor overtreden van de wet aangaande toestemmingsvereisten en daarmee en het grootschalig en structureel faciliteren van grootschalige datalekken aangaande uiterst gevoelige medische persoonsgegevens. Uiteraard dient ook de hoofdverantwoordelijke VZVZ te worden aangepakt en worden gedwongen om paal en perk te stellen aan de huidige illegale praktijken. Zowel door het verwijderen van (mogelijk) onterechte toestemmingen. Als door het verplicht aanbrengen van systeemwijzigingen waardoor het onmogelijk wordt om onterechte aanmeldingen te *kunnen* doen.

W.J. Jongejan

Plotse verschoning rechter daags voor rechtszaken aantasting beroepsgeheim en privacy

Uit welingelichte bron vernam ik heden dat op donderdag 1 december 2016 één van de rechters van de rechtbank Midden-Nederland bij het bureau wrakingen en verschoningen een verzoek tot verschoning heeft ingediend. Het betreft de rechter mevr. R.J. Praamstra, die op vrijdag 2 december in een meervoudige kamer met collegae twee zaken zou behandelen. Daardoor gaat de zitting niet door en volgt uitstel. De vereniging Vrijbit spant deze zaken aan tegen de Autoriteit Persoonsgegevens(AP). Het gaat om de zaken met kenmerken UTR 16/3326 en UTR 16/4199. In beide zaken draait het in de kern om de aantasting van het medisch beroepsgeheim en het fundamentele recht van patiënten op bescherming van hun privéleven. Deze zaken hebben zeer duidelijke raakvlakken met het wetsontwerp 33980 dat thans in de Eerste Kamer behandeld wordt. Waar gaat het om? Het gaat om een langlopende kwestie die gaat om de wijze waarop de AP, voorheen het College Bescherming Persoonsgegevens(CBP), haar rol vervult als toezichthouder, ten aanzien van handelen rond medische gegevens. Het lange beloop is voor een groot deel te wijten

aan de weigerachtige houding van de AP om op te treden tegen de wijze van handelen van zorgverzekeraars bij het inzien van medische gegevens bij zorgaanbieders.

Zaak UTR 16/3326 WBP V97

Inzet van het geding is de nalatigheid van de toezichthouder Autoriteit Persoonsgegevens om op te treden tegen de wijze waarop de zorgverzekeringsmaatschappijen in Nederland, volgens een gedragscode die in strijd is met zowel de Wet Bescherming persoonsgegevens(Wbp) als het Europees Verdrag voor de Rechten van de Mens (EVRM) verwerkingsprocedures hanteren aangaande de medische gegevens die zij verzamelen en verwerken.

Zaak UTR 16/4199 WBP V93

Inzet van dit geding is het plichtsverzuim van de toezichthouder om op te treden tegen de wijze waarop de Nederlandse Zorgautoriteit (NZa) medische diagnose- en behandelgegevens (DBC) van de gehele Nederlandse bevolking verzamelt, gebruikt en verstrekt aan derden. Namelijk via het Diagnose-Informatie Systeem (DIS) waar zorgverleners verplicht de DBC-gegevens voor dienen aan te leveren.

Weer vertraging

Het gevolg van het verschoningsverzoek nu is dat de behandeling van de beide zaken vertraging oploopt. Deze rechtszaken komen niet zo maar uit de lucht vallen en hebben een wat langere voorgeschiedenis. Op 13 november 2013 had de rechtbank Amsterdam al vernietigend geoordeeld over de goedkeuring die het CBP oorspronkelijk had gegeven aan de toentertijd door de zorgverzekeraars voorgestelde gedragscode omdat deze het medisch beroepsgeheim miskende en inbreuk maakt op de fundamentele bescherming van de privacy van patiënten. Dat komt omdat door de koppeling van de verwerking van medische persoonsgegevens aan uiteenlopende ‘bedrijfsprocessen’ als kwaliteitsbewaking, marketing en

zorgbemiddeling geen sprake is van de door het EVRM vereiste helder en limitatief omschreven doelstelling van gegevensverwerking, en de toetsing op proportionaliteit en subsidiariteit niet kan doorstaan. De rechtbank had daarbij uitdrukkelijk gewezen op de taak van het CBP als toezichthouder om ervoor te zorgen dat zorgverzekeraars zich houden aan de wettelijke kaders van de Wbp en EVRM; heel specifiek aan de wijze waarop eerdere rechterlijke uitspraken (van het College voor Beroep en bedrijf) daarbij hadden bepaald dat patiënten en zorgverleners nimmer gedwongen mogen worden om voor declaratiedoeleinden aan de verzekeraars vertrouwelijke diagnose-informatie af te staan.(tekst in hyperlink van Vrijbit)

Daarna heeft de AP, als opvolger van het CBP, lang getreuzeld met reageren.

Hinderlijk

Ronduit hinderlijk was de wijze waarop de geplande zitting van de zaak UTR 16/3326 WBP V97 op 30 september 2016 uitgesteld moest worden, omdat de AP na eerder door haar gevraagd uitstel niet tijdig de benodigde dossierstukken aanleverde. In een zo lang lopende zaak is het verre van professioneel als de vereiste stukken niet op tijd ingeleverd worden en riekt het naar obstructie.

Vraag

Het is raadselachtig waarom daags voor een zitting in een zo lang lopend juridisch gevecht in een principiële kwestie een rechter vraagt om niet opgesteld te worden. Het is de vraag of de betreffende rechter eigenstandig tot die beslissing gekomen is vanwege partijdigheid/nevenfunctie of dat de overige rechters hebben aangedrongen op het doen verschonen. Het trieste is dat het vragen van een rechterlijke uitspraak over het handelen of liever gezegd niet handelen van de AP zo een zeer moeizame zaak wordt.

In een democratische rechtsstaat moet het toch mogelijk zijn een toezichthouder ter verantwoording te roepen.

Want anders kan men zich alleen maar, met de dichter Juvenalis (ca. 60 – tussen 133 en 140 na Chr.), vertwijfeld afvragen: “ Quis custodiet ipsos custodes”

(*Wie zal de bewakers zelf bewaken?)*

W.J. Jongejan

Psychiatrie-afdeling UMCU balanceert op randje met big-data-analyse

Op 16 juli stond in het Financieel Dagblad(FD) een uitgebreid artikel van redacteur Marieke ten Katen met als titel: “Gedwongen opname? Op dag vijf zal de patiënt agressief zijn”. (1). Het gaat over de experimenten met big-data-analyse, die onder leiding van afdelingshoofd psychiatrie van het Universitair Medisch Centrum Utrecht(UMCU) Floor Scheepers(kinder – en jeugdpsychiater) sinds begin 2015

uitgevoerd worden met geanonimiseerde patiëntengegevens. Het betreft data uit 8000 patiëntendossiers. Het artikel vermeldt de steun van de Raad van Bestuur van het UMCU, met name van vicevoorzitter Frank Miedema. De initiatiefneemster is onder de indruk van de mogelijkheden van big-data-analyse en ziet mogelijkheden, voor de psychiatrie, maar ook voor chronische ziekten als kanker, ziekte van Parkinson en dementie om met big-data-analyse nieuwe wegen in te slaan. De doelstelling is om tot software te komen, die een risicoprofiel kan opstellen van een patiënt en ook een persoonlijke behandeling kan voorstellen. Het gaat dus om een vergaande vorm van "profiling". Profiling kent echter grote gevaren. Het belangrijkste gevaar is volgens Merel Eilander, woordvoerster bij de Autoriteit Persoonsgegevens, dat een patiënt anders wordt behandeld op grond van iets wat je zelf niet bepaald hebt of kunt controleren. Daarmee komt de individuele vrijheid in het geding. Software die drijft op de input van big-data zou een hulpmiddel moeten zijn, maar wordt in de praktijk vaak een alziend oog dat als vrijwel onfeilbaar beschouwd wordt. Teruggaand naar de titel van het artikel in het FD kan op basis van big-data-analyse daar eigenlijk alleen staan "Gedwongen opname? Op dag vijf **kan** de patiënt in vergelijking met andere dagen agressief zijn". De huidige titel straalt iets absoluuts uit.

Beperkingen

Binnen het UMCU realiseert men zich terdege dat er grote privacy-problemen ontstaan als de eigen geanonimiseerde database gekoppeld wordt aan andere databases met persoonsgegevens, zoals die van het Centraal Bureau voor de Statistiek(CBS). Koppeling van een database met geanonimiseerde of gepseudonimiseerde gegevens aan een andere met dezelfde voorzorgen kan bij voldoende dataoverlap en sophisticated software altijd leiden tot de mogelijkheid gegevens tot op een individu te herleiden. Daarom werd dat soort koppelingen tot nu toe in het UMCU nog niet tot stand

gebracht. Er wordt nu geanalyseerd met geanonimiseerde data op groepsniveau, **nog niet** op het niveau van individuele patiënten. Koppelingen voerde men uit met open databronnen, zoals gegevens over het weer(KNMI) of data over de buurt waar een patiënt woont. Daarbij kan je bij de eerste bron je nog wel voorstellen dat het uitvoerbaar is om met volledig geanonimiseerde data te werken. In het voorbeeld van de buurtdata moeten minimaal de vier cijfers van de postcode uitgesloten zijn geweest bij de anonimisering, omdat anders een koppeling met buurtdata onmogelijk zou zijn geweest.

Blijkbaar verloopt het onderzoek dat men nu doet met de koppeling aan open data-bronnen zonder toestemming van de patiënt. De initiatiefneemster stelt namelijk dat als er koppelingen zouden gaan plaatsvinden met bijvoorbeeld bepaalde CBS-gegevens toestemming van de patiënten nodig is, vanwege het herleidbaar worden van gegevens op individueel niveau. Dat is ook het officiële standpunt van de Autoriteit Persoonsgegevens(AP). Naar mijn idee dient echter elk onderzoek dat gebruikt maakt van patiëntgegevens aanleiding te zijn voor een gesprek met de patiënt, waarin men diens toestemming vraagt om de gegevens te verwerken.

Lastig

Het UMCU is in gesprek met juristen en patiënten en gaat **vooralsnog** niet over tot koppelingen aan andere databases met persoonsgegevens. Het wordt bij lezing van het artikel tussen de regels door wel als lastig ervaren. Dat woord neemt ook de jurist Maarten Goudsmit, werkzaam bij het grote advocatenkantoor Kennedy van der Laan halverwege het artikel in de mond. Deze verwijst ook naar uitspraak van de AP, waarin deze stelt dat medische gegevens moeilijk te anonimiseren zijn en dus toestemming aan de betrokken patiënten gevraagd moet worden. Bij een big-data-project vindt Goudsmit dat vragen om toestemming ronduit lastig. Hij schaart zich met dat standpunt automatisch bij de pro big-data lobby. De ondertoon bij dit deel van het artikel is duidelijk. De Wet bescherming

persoonsgegevens en de uitleg die de AP daaraan terecht geeft staat naar het oordeel van voorstanders van big-data-analyse ongelimiteerd gebruik van zorggegevens in de weg. In een eerder artikel legde ik uit dat aan de vereisten in het kader van de Wet bescherming persoonsgegevens, namelijk doelbinding, proportionaliteit en subsidiariteit bij big-data-analyse van zorggegevens eigenlijk nooit voldaan kan worden. Dat betekent ook weer niet dat daarom die wet daarom afgeschaft of veranderd moet worden.

Commercie

Dat de commercie zeer duidelijk geïnteresseerd is in deze schoorvoetende opening richting big-data-analyse blijkt wel uit de onbetaalde steun die volgens het artikel het UMCU kreeg van onder andere het data-adviesbureau GoDataDriven, dat meerdere hackathons organiseerde. Daarbij kijken datawetenschappers zonder medische achtergrond met grote inzet in een beperkte tijd(dag of weekend) naar data om te zien of er onvermoede verbanden te leggen zijn. GoDataDriven is zeker geen filantropische instelling. Op haar website wordt gewag gemaakt van projecten die liepen bij grote bedrijven als Bol.com, Wehkamp en Schiphol. Men zal alleen maar onbetaalde steun leveren als in de nabije toekomst toch commerciële opdrachten van het UMCU te verwachten zijn.

Oprekken

Het siert uitgerekend een afdeling psychiatrie van een universitair medisch centrum, die zeer privacygevoelige informatie onder haar beheer heeft, niet dat ze zelf het initiatief neemt voor enige vorm van big-data-analyse. Woorden als “nog niet” en “vooralsnog” wijzen op het willen doorzetten van de nu gepubliceerde intentie. In de wetenschap dat men direct dan wel indirect meewerkt aan het oprekken of ter discussie stellen van bestaande wet- en regelgeving over de bescherming van persoonsgegevens had een terughoudender opstelling van de afdeling psychiatrie en de raad van bestuur,

van meer wijsheid getoond. Per saldo legt men op deze wijze het vertrouwen van de patiënt, die de meest intieme zaken aan de arts c.q. de psychiater toevertrouwt, in de waagschaal. Men balanceert zo op de rand van de afgrond.

W.J. Jongejan

(1) Het artikel uit het Financieel Dagblad zit achter een betaalmuur, maar met een gratis registratie kunt u 5 artikelen per maand van het Financieel Dagblad gratis online inzien.

Autoriteit Persoonsgegevens ondergraaft stelselmatig eigen gezag

Het is opvallend hoe de Autoriteit Persoonsgegevens(AP), voorheen het College Bescherming Persoonsgegevens(CBP) al enige tijd opereert bij geconstateerde overtredingen. Ondanks het feit, dat die hebben plaatsgevonden is steevast het beleid om bij het beloven van beterschap geen sancties op te leggen. Volstaan wordt met de waarschuwing, dat het na beloofde verbeteringen niet weer mag gebeuren. Deze halfslachtige houding voedt de gedachte, dat de AP een toezichthouder is die de bij wet verkregen tanden(per 1 januari 2016 nog aangescherpt) niet wil laten zien door geen sancties op te

leggen. Daardoor ontstaat het beeld, dat de AP een verlengstuk is van de wetgever en uitsluitend de implementatie van wetten met zachte hand corrigeert en helpt uitvoeren. Ze wordt het verlengstuk van de politiek en geen krachtige, onafhankelijke, toezichthouder. Het speelt eigenlijk bij alle zaken die de AP onderzoekt, maar twee onderzoeken die van groot belang zijn voor de privacy van de burger, licht ik er voor u uit.

Suwinet

Dit is een besloten systeem waarmee verschillende overheidsorganisaties maatschappelijk gevoelige persoonsgegevens uitwisselen in het kader van werk en inkomen. Een onderdeel van het UWV (Uitvoerings-instituut WerknemersVerzekeringen) ondersteunt, beheert en ontwikkelt het verder. Via diverse applicaties bestaat toegang tot (persoons)gegevens van burgers, waaronder financiële data. De bronhouders van de gegevens zijn onder andere de Gemeentelijke Sociale Diensten, het UWV en de Sociale VerzekeringsBank, maar ook de belastingdienst en de rijksdienst voor het wegverkeer. Naast deze partijen hebben ook de Immigratie- en NaturalisatieDienst, de Inspectie SZW, gemeentelijke belastingdeurwaarders, gemeenten in het kader van de meld- en coördinatiepunten voortijdig schoolverlaters en de Stichting Netwerk Gerechtsdeurwaarders toegang tot het netwerk. Er zijn veel protocollen en richtlijnen voor de toegang gemaakt, maar daar bleek een meerderheid van de gemeenten zich niet aan te houden. Mensen die geen toegang zouden moeten hebben tot het systeem kregen dat wel, ook personeel van externe bureaus, die door gemeenten ingehuurd waren. Ook werd het Suwinet in enkele gevallen gebruikt voor een ambtelijk doel waarvoor het niet opgezet was, namelijk het parkeerbeheer. Veel overtredingen constateerde de AP bij onderzoek. Op 21 januari 2016 verscheen dat rapport over overtredingen bij 11 van de 13 onderzochte gemeenten. Wat gebeurt er? De AP maant de overtreders, volgt ze door een vervolgonderzoek te doen, maar legt geen enkele sanctie op aan de overtreders, die geacht werden te weten hoe

het wel zou moeten.

DIS

De afgelopen jaar heeft de AP zich ook beziggehouden met de rechtmatigheid van het doorleveren van gegevens uit het DBC-Informatie Systeem(DIS) door de Nederlandse Zorgautoriteit(NZa) aan derden. Nadat eerst de organisatie DBC-onderhoud de verantwoordelijkheid droeg voor het DIS werd op 1 mei 2015 die verantwoordelijkheid ondergebracht bij de NZa. Het ging om ge-pseudonimiseerde zorggegevens, die bij nadere beschouwing toch herleidbaar waren tot individuen. De AP was tot dat onderzoek min of meer gedwongen door publiciteit omtrent de herleidbaarheid. De AP was al eerder op de hoogte van deze materie o.a. door de uitzending van de tv-rubriek Zembla in 2014. Het komt uiteindelijk tot een uitspraak van de AP over dit onderwerp op 7 maart 2016. Daarin zegt de AP dat de gegevensverzameling van het DIS op zich wel rechtmatig is, maar dat doorlevering aan derden, zoals bijvoorbeeld de minister van VWS en het Centraal PlanBureau niet rechtmatig is. Het conceptrapport legde de AP eerst aan de NZa voor en paste het na een reactie van de NZa alsnog aan. Hoor en wederhoor bij mogelijke overtredingen hoort er te zijn, maar dat hoort plaats te hebben voor enig rapport uitgebracht wordt. Het voorleggen van een concept-rapport aan een onderzochte instantie is in mijn ogen al een zwaktebod. En wat gebeurt er met de geconstateerde overtredingen. De NZa belooft het niet meer te doen. De AP heeft daar vervolgens vrede mee ZONDER sancties op te leggen vanwege de begane overtredingen.

Vergelijking

De handelswijze van de AP ten aanzien van geconstateerde overtredingen is heel vreemd. Het is hetzelfde als wanneer een dief betrapt is op een serie diefstallen, belooft het niet meer te doen en vervolgens geen straf krijgt opgelegd.. De handelswijze van de AP strookt absoluut niet met het

rechtsgevoel, omdat organisaties waar de AP toezicht op houdt zo altijd wegkomen bij overtredingen zonder sancties. Het is bijvoorbeeld bij de Autoriteit Financiële Markten(AFM) niet voor te stellen, dat een overtreder met de belofte het nooit meer te doen geen sanctie opgelegd krijgt.

Uiteindelijk ondergraaft deze uiterst zwakke handelswijze van de AP het vertrouwen van de burgers in de overheid. Een sterke en ferm optredende toezichthouder is in het belang van burger en overheid.

Zachte heelmeesters maken nu eenmaal stinkende wonden.

W. J. Jongejan

Opt-in-vraag LSP door thuiszorg strijdig met Wbp

Recent schreef ik op deze website een artikel over het gaan vragen door thuiszorgmedewerkers van de opt-in-toestemming voor elektronische gegevensuitwisseling via het Landelijk SchakelPunt(LSP). Hierin gaf ik aan dat het vragen van deze toestemming, door een ander dan de brondossierhouder onfatsoenlijk, ongewenst en illegaal is. In Nijmegen is een taskforce om het aantal opt-in-toestemmingen te maximaliseren aan de slag gegaan met het idee de thuiszorg daarbij in te

schakelen. Bij bestudering van wat in de Wet bescherming persoonsgegevens(Wbp) staat en de uitleg die de Autoriteit Persoonsgegevens(AP) daarbij geeft is duidelijk dat als de opt-in-toestemming verkregen wordt bij een ander dan de brondossierhouder er sprake is van overtreding van artikel 33 en 34 van de Wbp. Van deze overtreding is door mij melding gemaakt bij de Autoriteit Persoonsgegevens. Op 18 juli berichtte de AP dat de brief daarover in goede orde ontvangen was.

Wetsartikelen

Hoofdstuk vijf van de Wbp gaat over de informatieverstrekking aan de betrokkene(patiënt) en de meldplicht bij inbreuken op de beveiliging van persoonsgegevens aan het College. Met College wordt het College Bescherming Persoonsgegevens(CBP) bedoeld, de rechtsvoorganger van de Autoriteit Persoonsgegevens(AP). In de artikelen 33 en 34 wordt duidelijk omschreven dat de verantwoordelijke(de brondossierhouder in dit geval, dus de huisarts of apotheker) vóór de verwerking van de gegevens de betrokkene(de patiënt) voorlicht om die geggevens daarna(met toestemming van de patiënt) te verwerken. Artikel 34 lid 4 kan bij de LSP-opt-in niet van toepassing zijn. Daar staat een uitzondering voor het geval het verkrijgen van de toestemming een onevenredige moeite zou kosten. Dat is niet het geval want voor het Nijmeegse initiatief was er in die regio al een redelijk toestemmingspercentage.

De tekst van de artikelen luidt:

Artikel 33

1. Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij de betrokkene daarvan reeds op de hoogte is.

2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mede.
3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Artikel 34

1. Indien persoonsgegevens worden verkregen op een andere wijze dan bedoeld in artikel 33, deelt de verantwoordelijke de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij deze reeds daarvan op de hoogte is: **a.** op het moment van vastlegging van hem betreffende gegevens, of **b.** wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.
2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking mede.
3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.
4. Het eerste lid is niet van toepassing indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast.
5. Het eerste lid is evenmin van toepassing indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te

informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid.

Uitleg AP

Op de website van de Autoriteit Persoonsgegevens kan men ook een duidelijke uitleg vinden van wat in artikel 33 en 34 Wbp staat. Deze uitleg sluit ook uit dat een ander dan de brondossierhouder een opt-in-toestemming voor elektronische gegevensuitwisseling via het LSP vraagt. Het is alleen bij de AP de vraag of deze door de politiek bewust onderbemande dienst met een veel te laag budget het handhaven in deze kwestie ook ter hand neemt.

Thuiszorg

Hoewel de thuiszorgorganisaties in 2015 reeds in de koepeladviesraad van de Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ), als beheerder van het LSP, zijn opgenomen, is er geen sprake van het bijhouden van een aan het LSP gekoppeld brondossier bij die organisaties. Bij veldproeven in de regio Dordrecht/Gorinchem bleek dat het werken met het LSP in pilot-verband niet goed verliep. Daarbij kon bij de thuiszorgorganisatie de daar verantwoordelijke arts ouderenzorg alleen maar een medicatieoverzicht opvragen zonder eigen data via het LSP aan te kunnen leveren. Datgene wat geprobeerd werd lukte slecht en stuitte op grote mandateringsproblemen, waardoor men er mee stopte. Het opgenomen zijn in de koepeladviesraad van VZVZ zegt dan ook totaal niets over het gekoppeld zijn van thuiszorgsystemen aan het LSP.

De aanwezigheid in de koepeladviesraad kan dus nooit een legitimatie zijn voor hetgeen de taskforce in Nijmegen nu uitvoert. Ik ben zeer benieuwd of de AP hier actief gaat handhaven. De AP is het wel aan zijn stand verplicht dit te doen.

W.J. Jongejan