Contraterrorisme mbv gezondheidszorg. Verwerpelijke MEDINT in de NHS

Recent werd ik attent gemaakt op een publicatie in het online magazine Security Dialogue, geschreven door Charlotte Heath-Kelly, assistent professor van het Department of Politics and International Studies van de University of Warwick in het Verenigd Koninkrijk. De titel was "Algorithmic autoimmunity in the NHS(National Health Service): Radicalisation and the clinic". Het is een artikel ,dat door het abstracte taalgebruik wat lastig toegankelijk is, maar glashelder wat betreft de boodschap. De kern van het stuk is dat in het Verenigd Koninkrijk werkers in de gezondheidszorg, zoals optometristen, tandartsen, dokters en verpleegkundigen verplicht en getraind zijn tekenen van radicalisatie te rapporteren aan de autoriteiten in het kader van het bestrijden van terrorisme. Het is een zeer discutabele vorm van Medical Intelligence(MEDINT). De regering van het Verenigd Koninkrijk heeft die keuze expliciet gemaakt vanwege de grote aantallen mensen uit de hele bevolking, die in contact komen met gezondheidszorg-werkers. Het is een strategie die in officieel in 2011 geformuleerd is en die sindsdien ten uitvoer is gebracht met een verplichting tot medewerking in 2015. De strategie is bedacht door het Home Department(het ministerie van binnenlandse zaken) en destijds ten uitvoer gebracht onder

leiding van Theresa May, de huidige minister-president.

Prevent-programma

Het Prevent-programma is officieel in 2011 bediscussieerd en gepubliceerd, maar was in het geheim al veel langer actief. Al in 2003 begon de regering ermee als een post 9/11-strategie, maar hield het lage tijd geheim. Onder de naam Contest, was het in regeringskringen bekend met een opzet die beruste op 4 P's: "Prepare for attacks, Protect the public, Pursue the attackers and Prevent their radicalisation to start with." In 2010 werd bekend dat in meerdere, door veel moslims bevolkte wijken van Birmingham, heimelijk bewakingscamera's waren geplaatst, betaald door het Home department. Dat was uitgevoerd met geld voor terrorismebestrijding. Onder andere daardoor zijn in 2010 openlijke discussies gestart die toen het openlijke Prevent-programma opleverden. In de Prevent-stukken noemt men niet alleen al-Qaeda-terreur of ander moslimextremisme als te bestrijden doelen, maar ook vormen van rechts-extremisme.

Verplicht

In 2015 is krachtens de Counter-Terrorism and Security Act deelname aan het Prevent-programma verplicht gesteld("statutory obligation') in sectie 26 van deze wet. Deelname door NHS in Schedule 6 in de alinea "Health and social care". Door het in werking treden van deze wet is verscheen ook een Revised Duty Guidance van het Prevent-programma, waarin de plichten nog weer eens uitgelegd werden. Hoe het in de praktijk in onderdelen van de NHS geïmplementeerd diende te worden ziet u hier.

Uitgangspunt

De basis waar men van uit gaat bij het inschakelen van zorgmedewerkers aldus verwoord in de Prevent-Strategy:

“10.143 Given the very high numbers of people who come into contact with health professionals in this country, the sector is a critical partner in Prevent. There are clearly many opportunities for doctors, nurses and other staff to help protect people from radicalisation. The key challenge is to ensure that healthcare workers can identify the signs that someone is vulnerable to radicalisation, interpret those signs correctly and access the relevant support”

En:

“10.145 The Department of Health will need to ensure that the crucial relationship of trust and confidence between patient and clinician is balanced with the clinician’s professional duty of care and their responsibility to protect wider public safety. Where a healthcare worker – be that a speech therapist, community psychiatric nurse or general practitioner – encounters someone who may be in the process of being radicalised towards terrorism, it is critical that the individual is offered the appropriate support. We believe that clear guidelines are needed for all healthcare managers and healthcare workers to ensure that cases of radicalisation whether among staff or patients are given the attention and care they deserve.”

Uit de laatste zin wordt duidelijk dat patiënten niet de enige doelgroep zijn waarover men rapportage wenst, maar ook over stafleden, eigen collegae.

Opzet binnen NHS

Het betrekken van zorgaanbieders binnen de NHS had en heeft ten doel om radicalisatie van burgers op te sporen om daarmee de samenleving te beschermen. Daartoe vindt een specifieke training plaats van medisch personeel. Bij die training krijgt de betrokkene een Powerpoint-presentatie met 41 slides te zien, waarin de zorgplicht jegens kwetsbare kinderen en volwassenen benadrukt wordt. Daarbij vinden ook testen, in de

vorm van multiple-choice-vragen plaats, over de wijze waarop de gewenste informatie aan managers moet worden gemeld. Wat men wil is dat dat zorgmedewerkers melden op basis van "intuïtie" en niet zozeer op basis van een aantal tevoren vastgestelde criteria.

Stilte in NHS

In een artikel van de journaliste Anne Gulland in de British Medical Journal dat op 26 april 2017 verscheen, vraagt zij zich hardop af waarom het verplicht meewerken met het Prevent-programma in het onderwijs meer onrust veroorzaakte dan in de zorg. Zij maakt wel melding van een gering aantal meldingen aan de bevoegde autoriteiten. In een bespreking van dit artikel op een online nieuwsmagazine van de American Association for the Advancement of Science is nog duidelijker te lezen hoe de medewerking is binnen de NHS.

Volkomen verkeerde weg

Het is naar mijn mening ongekend dat gezondheidszorgwerkers in een dergelijk mate ingeschakeld worden bij politionele activiteiten. De voornaamste reden dat men in het Verenigd Koninkrijk zover heeft kunnen en willen gaan, lijkt me gelegen in het feit dat het gaat om een door de staat betaald en georganiseerd zorgstelsel. Daarin is degene die betaalt degene die bepaalt.

In eigen land heeft Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in de Nationale Contraterrorismestrategie 2016-2020 het over contacten met een breed scala aan partners, waaronder de jeugdzorg en GGZ(op pag. 9 en 13 van het document). Ziekenhuiszorg of huisartsenzorg worden niet genoemd.

Vertrouwen

Bij het bezoek aan een gezondheidszorgwerker, waaronder artsen dient de vertrouwelijkheid van wat gezegd is en wat gebeurt in

de spreekkamer voorop te staan. Het is de basis van het medisch beroepsgeheim. Het geïnstitutionaliseerd melden van observaties, gebaseerd op “intuïtie”, is een volkomen verkeerde weg die begaan wordt. Bij het in de breedte bekend worden van deze activiteiten door zorgmedewerkers zal dit gaan lijden tot zorgmijden en daardoor extra gevaren voor de volksgezondheid.

Als een arts of andere zorgwerker iets crimineels verneemt wat kan lijden tot een groot gevaar voor één of meerdere personen kan hij/zij in Nederland altijd daarvan bij de bevoegde instanties melding maken op basis van een conflict van plichten. Overigens is het altijd verstandig om in zulke gevallen eerst ruggenspraak te houden met advocaten van de eigen beroepsorganisatie of KNMG.

W.J. Jongejan

Het artikel van Charlotte Heath-Kelly is toegankelijk door publicatie op het Sagepub-platform.

Bizarre uitspraak namens SBG tijdens kort geding over verantwoordelijkheid patiënt

Tijdens het kort geding tegen de Stichting Benchmark GGZ(SBG), dat op 13 juli j.l. diende voor de Rechtbank Midden-Nederland deed de advocaat van de SBG een wel zeer bijzondere uitspraak over de verantwoordelijkheid van de patiënt. De inzet van het geding was om het verwerken door de SBG van patiëntgegevens(ROM-data) voor het benchmarken(vergelijken van zorgaanbieders) te doen stoppen. Reden voor dat laatste is het feit dat de gegevens veelal zonder toestemming van de patiënt verzameld zijn door de SBG. Zelfs de minister van VWS moest erkennen dat de data illegaal verzameld waren. Bij het voorlezen van de pleitnota door de advocaat van de SBG, afkomstig van het advocatenkantoor Kneppelhout & Korthals, deed deze een zeer opmerkelijke uitspraak die aangeeft dat de SBG een zeer gebrekkige kennis heeft van wetgeving en patiënten-rechten.

Uitspraak

Wat zei de advocaat van de SBG precies:

"Niet betwist wordt immers, ***dat de patiënt de ethische verantwoordelijkheid heeft aan een lerend zorgsysteem bij te dragen.*** *En dus ook aan de ontwikkeling van ROM door middel van benchmarking. Het doel van ROM is immers drieledig: dat de patiënt profiteert, andere patiënten profiteren en het zorg(kwaliteitssysteem) profiteert. Niet meewerken is dus anti-solidair of….. niet ethisch!"*

Wet

Omdat de ROM-data die de SBG verzameld ondanks (dubbel)

pseudonimiseren toch als bijzondere persoonsgegevens beschouwd moeten worden, is voor het verzamelen daarvan uitdrukkelijke toestemming van de patiënt nodig. Dat staat in artikel 23 van de Wet bescherming persoonsgegevens(Wbp). Het toestemming vragen is bij het verzamelen van de ROM-data door de SBG niet gebeurd, waardoor zelfs de minister van VWS moest erkennen dat zoiets niet legitiem is. Het is een recht van de patiënt om te weigeren toestemming te geven om ROM-data van hem/haar naar de SBG te sturen. De uitspraak namens de SBG ontkent het bestaan van patiëntenrechten. Het is dus volledig buiten de orde om het verzamelen van de ROM-data te vergoelijken door te stellen dat het een "ethische" verplichting is om aan een lerend zorgsysteem bij te dragen.

Gotspe

Het zotte van deze redenatie is dat op deze wijze elke niet legitieme verzameling van medische gegevens van patiënten, wat ze ook mankeren, goed te praten zou zijn op basis van een "ethische verantwoordelijkheid" om mee te werken door de patiënt. Ook zou het dan toepasselijk zijn voor het meewerken aan systemen die nog bezig zijn de niet legitiem verkregen informatie geschikt te maken om er eventueel conclusies uit te trekken. Want dat is precies van de SBG doet: het door-ontwikkelen van de ROM-data-verwerking omdat de ROM-data eigenlijk helemaal niet geschikt en bedoeld zijn voorbenchmarking en zorginkoop. De SBG verzorgt dat, volledig betaald door Zorgverzekeraars Nederland(ZN).

Truc

Door in de pleitnota te zetten dat deze redenatie niet betwist wordt door de advocaat van de eisers in het kort geding, de actiegroep StopBenchmarkROM en twee patiënten waarvan data illegitiem verzameld waren, gebruikte de advocaat van de SBG een wel heel zwakke truc. In het kort geding werd de rechtmatigheid van het handelen van de SBG betwist ten aanzien van het verzamelen van ROM-data en niet een door de SBG of

haar advocaten bedachte “ethische verantwoordelijkheid” van de patiënt om mee te moeten doen.

Sneu

Als tranentrekker bedoeld kwam de advocaat van de SBG met de opmerking richting de rechter dat als de SBG niet door mocht gaan met haar ROM-data-verzamelen er 14 personen werkloos zouden raken. Dat is op zijn zachtst gezegd wel heel erg doorzichtig en sneu als men bedenkt dat twee dagen voor de rechtszitting de bestuurspartijen van SBG, te weten GGZ Nederland, Zorgverzekeraars Nederland en MIND kenbaar maakten dat de SBG op zal gaan in een nieuw op te richten KwaliteitsInstituut voor de GGZ. De SBG zal daar een significante bijdrage aan leveren qua kennis en mankracht. De advocaat van de SBG kwam dus met een inhoudsloos argument.

Duidelijk

Met de door de SBG gesanctioneerde uitspraak tijdens het kort geding wordt andermaal duidelijk hoe door deze stichting, maar veel belangrijker, door Zorgverzekeraars Nederland als financier van de SBG, aangekeken wordt tegen het verzamelen van patiëntgegevens. Alles moet blijkbaar wijken om gegevens in handen te krijgen die te gebruiken zijn bij zorginkoop. Het woord kwaliteitsbewaking is daarbij een soort schaamlap die de dienstbaarheid aan zorginkoop moet verhullen.

W.J. Jongejan

VZVZ inventariseert LSP-

weigerende huisartsen per telefoon

Zeer recent vernam ik van één van de niet op het Landelijk SchakelPunt(LSP) aangesloten huisartsen dat zijn assistente uitgebreid via de telefoon benaderd was door een medewerker van VZVZ. Dat is de Vereniging van Zorgaanbieders Voor Zorgcommunicatie die verantwoordelijk is voor het beheer en gebruik van het LSP. In het telefoongesprek in opdracht van één van de implementatiemanagers van VZVZ zei men te willen inventariseren wat de reden(en) zijn voor het niet aansluiten op het LSP. Nu is dat op zijn zachtst gezegd het intrappen van een open deur, want na ongeveer vijf en een half jaar voortmodderen met het LSP is het wel duidelijk dat de weigerende huisartsen dat niet om praktische maar om principiële redenen niet aangesloten zijn. Tot nu toe is 91 procent van de huisartspraktijken aangesloten op het LSP. De negen procent weigeraars zijn de harde kern van praktijkhouders die geen brood zien in communicatie van medische data via het LSP. Aansluiting door praktijkhouders is een vrijwillige zaak evenals het toestemming verlenen door de patiënt om medische data te doen delen.

Opzichtig

In het licht van het bovenstaande is het nogal opzichtig dat de weigerachtige huisartsen benaderd worden met de vraag waarom zij het niet willen. Daarnaast is het nogal apart om

met die vraag de praktijkassistente telefonisch te benaderen. Blijkbaar is men op zoek naar een "soft spot" binnen de praktijken om aldaar een discussie op gang te brengen over het niet-aangesloten zijn. Na het telefoongesprek kreeg de huisarts nog een email toegestuurd met de mededeling dat zijn assistente benaderd was met onder andere de vraag of er een speciale reden was waarom de praktijk nog niet aangesloten is op het LSP. In de email werd die vraag hem ook gesteld. Hij kreeg ongevraagd het aanbod om een afspraak te maken met een implementatiemanager van VZVZ om zo begeleiding te krijgen bij het aansluiten. Er moeten bij VZVZ meerdere van dit soort functionarissen in dienst zijn.

Sociale druk en ontzorgen

Wat VZVZ met dit soort acties doet, past precies in een strategie die door twee sociologen van de Universiteit van Amsterdam(UvA) in 2016 in een publicatie geanalyseerd en uitgelegd is. Tim ten Ham en Christian Broër schreven dit in een artikel, genaamd Risico's vermijden door depolitisering, dat in 2016 verscheen in het online magazine Sociology. Ik schreef er op 15 juli 2017 een artikel over. Eén van de implementatietechnieken die VZVZ inzet is het verleiden van zorgverleners en het wegnemen van principiële bezwaren. Hiervoor maakt zij gebruik van retorische middelen die zorgverleners bewust moeten maken van de voordelen van het LSP. Ook gebruikt men emotiemanagement om de gevoelens van de zorgverleners te beïnvloeden. Gewezen wordt dan op het kleine deel dat nog weigert en dat het daardoor gênant is om anno 2017 niet aangesloten te zijn op het LSP. Dat wordt onder andere bewerkstelligt door het inschakelen van "ambassadeurs". Dat zijn zorgverleners die wel aangesloten zijn en een beroep op hun collegae moeten doen onder andere met de argumentatie dat men zich moet schamen voor de collegae en patiënten dat ze nog niet aangesloten zijn. Tegelijkertijd komt VZVZ dan met een aanbod om het aansluiten te "ontzorgen" door het aanbieden van hulp door een implementatiemanager.

Weerstandsnesten

Door opbelactie van VZVZ wordt duidelijk dat men daar de niet aangeslotenen ziet als weerstandsnesten die opgeruimd moeten worden. Noch bij de huisartsen, noch bij de apothekers, huisartsenposten of ziekenhuizen is een aansluitingspercentage van honderd procent gehaald. Wat een veel groter probleem voor VZVZ is dat het aantal opt-in-toestemmingen van burgers voor het doen delen van hun medische informatie bij huisartsen. Nog steeds heeft slechts 35 % van de Nederlanders daar toestemming voor gegeven. Dat percentage is de laatste twee jaar nauwelijks gestegen.

Subtiel

VZVZ blijkt dus op dit moment op subtiele wijze bezig huisartspraktijken onder druk te zetten om aan te sluiten. Na vijf en een half jaar LSP in private handen mag het toch wel als bekend worden verondersteld dat de niet-aangeslotenen principiële weigeraars zijn. Mocht u tot die laatste groep behoren, kijk dan niet vreemd op als uw assistente of uzelf, als weigeraar, opeens gebeld wordt door het implementatiemanagement van VZVZ, bijv. Kars Hillenius of Cindy Koolhaas.

W.J. Jongejan

Nieuwe wet staat aantasting beroepseed artsen toe. Oproep

aan KNMG

Op dinsdag 11 juli 2017 is in de Eerste Kamer het wetsontwerp 34588 aangenomen, voluit het voorstel van wet houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2002). Hierin zijn vergaande nieuwe bevoegdheden van de Algemene Inlichtingen en Veiligheids-Dienst(AIVD) en de Militaire Inlichtingen en Veiligheidsdienst(MIVD) opgenomen. Die gaan van de uitbreiding van tapmogelijkheden, via het vergaand afluisteren van het internet tot het actief hacken van verdachten en zijn omgeving. De formulering van het aangenomen wetsontwerp is zodanig dat het niet uitgesloten is dat de veiligheidsdiensten zich toegang verschaffen tot ICT-systemen met medische informatie of medische netwerken. Het bewaren van het medisch beroepsgeheim is daardoor in het geding. Na het aannemen van het wetsvoorstel door de Eerste kamer heeft een brede coalitie van juristen, journalisten, privacy-organisaties en tech-bedrijven aangekondigd zich niet neer te leggen bij de goedkeuring door de Eerste Kamer. Deze groep, geleid door het Public Interest Litigation Project(PILP) stapt naar de rechter in de hoop dat die een stokje steekt voor de aftapwet. Eventueel zal door geprocedeerd gaan worden tot aan het Europese Hof van Justitie en het Europese Hof voor de Rechten van de Mens. De Koninklijke Nederlandse Maatschappij ter bevordering van de Geneeskunst(KNMG) zou zich in het kader van het bewaken en beschermen van het medisch beroepsgeheim dienen aan te sluiten bij dit initiatief om te voorkomen dat

inlichtingendiensten toegang krijgen tot medische computersystemen of medische netwerken.

Toetsing

Op papier dient er toetsing plaats te vinden door een Toetsingscommissie Inzet bevoegdheden(TIB) die weer valt onder een toezichthouder, de Commissie van Toezicht op de Inlichtingen- en Veilig-heidsDiensten(CTIVD). Het voorbeeld van de V.S. waarbij veiligheidsdiensten via een speciaal ge-rechtshof toestemming dienen te vragen voor bijzondere opsporingsvragen, het United States Foreign Intelligence Surveillance Court, laat zien dat zoiets een wassen neus is. Het wordt daar eigenlijk nooit geweigerd.

MEDINT

Onder het begrip MEDINT(Medical Intelligence) verstaan veiligheidsdiensten inlichtingen op medisch gebied, maar ook niet-medische informatie die via medische dossiers verkregen kan worden, zoals adressen, verzekeringsnummer, etc. Ook in Nederland leeft het willen inzien van medische systemen en medische netwerken. Na de aanslagen in Parijs in 2016 liet het oud-hoofd van de MIVD, Peter Cobelens op de televisie duidelijk weten dat die ambitie er wel degelijk is. In het nu aangenomen wetsontwerp is er geen uitzondering gemaakt voor medische systemen en netwerken, zelfs niet voor medische apparatuur, die in het lichaam van een burger is ingebracht, zoals pacemakers, inwendige defibrillatoren etc. Dat laatste probeerde het D66 Tweede Kamerlid Kees Verhoeven te voorkomen door een amendement op artikel 45 van het wetsontwerp in te dienen. Dat amendement werd echter op 14 februari 2017 verworpen.

LSP niet uitgesloten

In het aangenomen wetsontwerp staat nadrukkelijk het benaderen van systemen en netwerken. Medische informatie wordt over diverse netwerken uitgewisseld. Eén daarvan is het systeem

waar het Landelijk SchakelPunt(LSP) het centrale punt is. Omdat een Amerikaanse leverancier, CSC, het LSP gemaakt heeft en onderhoudt kan met een beroep op de Patriot Act door Amerikaanse diensten inzage afgedwongen worden. Thans maakt ook onze eigen nationale wetgeving inbreuken op het systeem mogelijk.

Hoe?

In de pers is ruimschoots duidelijk geworden dat veiligheidsdiensten vaak gebruik maken van zwakheden in systemen. Eén voorbeeld daarvan zijn de zogenaamde zero-day-hacks. Dit zijn hacks op basis van fouten in besturingssystemen of programma's die nog niet algemeen bekend zijn en waarvoor de fabrikant nog geen update of patch gemaakt heeft. Het kan uitermate gevaarlijk zijn om de IT-systemen niet veiliger te maken door de gaten in de software te laten voortbestaan, bijvoorbeeld door updates van het besturingssysteem niet meteen of niet automatisch te installeren. Overigens gaat het om alle systemen: databases, mails, maar ook medische apparaten, en mobiele telefoons gebruikt door medici en hun ondersteunend personeel. Dat heeft de golf van geblokkeerde (medische) systemen met de Wannacry-malware laten zien.

KNMG

In een ingezonden artikel in het NRC-Handelsblad op 4 maart 2016 waarschuwden de schrijvers al voor het hacken van medische systemen en netwerken door onder andere nationale veiligheids-diensten. Toen was het onderhavige wetsontwerp nog onder behandeling in de Tweede Kamer. Het grote probleem is dat als artsen niet meer in kunnen staan voor de bescherming van patiëntgegevens de Eed van Hippocrates tot een dode letter verwordt. De aangenomen wet maakt schending van het beroepsgeheim mogelijk. Het wordt thans tijd dat de KNMG duidelijk maakt dat wat haar betreft de grens overschreden is.

De KNMG zou zich moeten aansluiten bij de brede coalitie, die via de rechter alsnog probeert de wet niet tot uitvoer te doen brengen om zo het medisch beroepsgeheim te beschermen.

Wij roepen de KNMG daartoe op, omdat met de nieuwe wet op de veiligheidsdiensten medische informatie vogelvrij is verklaard!

W.J. Jongejan en G. Freriks

Wim J. Jongejan was van 1976 tot 2007 huisarts en volgt intensief zorg-ICT en privacy-zaken in de zorg. Gerard Freriks is arts en was betrokken bij het maken van een standaard voor informatiebeveiliging in de zorg (NEN7510).

Rechtbank maakt gehakt van opvatting Stichting Benchmark GGZ over Btw-betaling

Uitgerekend op de dag dat het kort geding van de actiegroep Stop Benchmark ROM tegen de Stichting Benchmark GGZ (SBG) in Utrecht diende, donderdag 13 juli 2017, deed de Rechtbank Gelderland uitspraak in twee zeer opvallende zaken (AWB 16/2863 en AWB 16/2862). Het betreft een conflict tussen de

belastingdienst en SBG over het afdragen van Btw door de SBG over door haar verleende diensten. Eiser was niet de belastingdienst, kantoor Utrecht, maar de SBG die beroep instelde na het afwijzen van een bezwaar. De SBG was namelijk van mening dat over haar werkzaamheden geen Btw verschuldigd was. De uitspraak van de meervoudige kamer van de Rechtbank Gelderland was dat het beroep ongegrond werd verklaard. Het bijzondere aan deze zaak is dat de rechters heel gedecideerd vonnisten over een op zijn zachtst gezegd toch wel trieste en gênante redenatie van de SBG. Die redenatie betrof naast de gedachte dat de SBG geen onderneming zou zijn in de zin der wet, en zij bovendien zou vallen onder een aantal vrijstellingen van Btw-betaling. Puntsgewijs zal ik daarop ingaan.

Twistpunt

Zoals gezegd was het twistpunt het al dan niet betalen van Btw. De belastingdienst had over het derde kwartaal 2011 een aanslag van € 43.046 aan Btw opgelegd. Op jaarbasis zou dat € 172.184 zijn. De SBG was het daar niet mee eens. Ze is in 2011 opgericht en zegt als doelstelling te hebben het zonder winstoogmerk als een 'trusted third party' voor de geestelijke gezondheidszorg(GGZ) te benchmarken op het gebied van behandeleffect en klanttevredenheid. Voor de duidelijk zij vermeld dat de SBG volledig door Zorgverzekeraars Nederland(ZN) gefinancierd wordt. Voor 2011 en 2012 ging dat om 2,2 miljoen euro per jaar.

Onderneming

De rechtbank was het volledig oneens met de opvatting dat de SBG geen onderneming zou zijn. De rechters oordeelden dan ook dat het een dienstverlenende onderneming is die gewoon Btw-plichtig is over de verleende diensten. De stelling van de SBG dat zij geen winst beoogt en geen commerciële nevenactiviteiten mag verrichten maakt het voorgaande niet anders.

Sociaal-culturele vrijstelling

De SBG beriep zich op de toepasselijkheid van sociaal-culturele vrijstelling voor het betalen van omzetbelasting. De rechtbank oordeelde dat de SBG geen erkenning had als instelling van sociale aard en dat haar diensten niet nauw samenhangen met de sociale zekerheid. Daarom oordeelden de rechters ook negatief over vrijstelling op genoemde gronden. Het is niet goed te begrijpen waarom de SBG een beroep deed op deze vrijstelling.

Koepel-vrijstelling

De SBG redeneerde ten aanzien van dit punt als volgt. Zij verricht diensten voor zorginstellingen en zorgverzekeraars en beschouwt deze als leden van de koepel. Naar het oordeel van de rechtbank zijn de prestaties van de SBG niet rechtstreeks nodig voor het verrichten van de prestaties door de zorginstellingen en de zorgverzekeraars. De rechters komen dan ook tot de conclusie dat de koepelvrijstelling niet van toepassing is, omdat de diensten van de SBG niet rechtstreeks nodig zijn voor de prestaties van de zorginstellingen en de zorgverzekeraars.

Kwaliteit

Over de claim van het werken aan kwaliteitsverbetering in de GGZ doet de rechter een bijzondere en belangwekkende uitspraak. Hier zegt de rechtbank:

“Hoewel kwaliteitsbewaking van de ggz rechtstreeks nodig is voor de prestaties van de zorginstellingen en daarvoor onontbeerlijk is, kan ditzelfde niet worden gezegd van benchmarking. Dat zorginstellingen de benchmarkprestatie afnemen omdat zij met behulp daarvan aan kwaliteitsbewaking willen doen is niet voldoende. Die kwaliteit kan ook op andere wijzen bewaakt worden. Naar het oordeel van de rechtbank kan niet gezegd worden dat de zorginstellingen niet dezelfde mate of kwaliteit van gezondheidszorg zouden kunnen leveren zonder

gebruik te maken van benchmarking. Verweerder heeft terecht opgemerkt dat andere wijzen van kwaliteitstoetsing, zoals intercollegiaal overleg, evenzeer een bijdrage aan kwaliteit leveren.”

Medische vrijstelling

Ronduit gênant wordt het als de SBG vrijstelling van omzetbelasting vraagt op medische gronden. Ze deed daarbij een beroep op artikel 11, eerste lid, aanhef en onder c, van de Wet OB en artikel 132 eerste lid, aanhef en onder b, van de Btw-richtlijn. Artikel 11 houdt in dat men zich bezighoudt met het verzorgen en verplegen van een in instelling opgenomen personen, alsmede handelingen die daar nauw mee samenhangen zoals het verstrekken van spijzen, dranken, medicijnen etc. Artikel 132 van de Btw-richtlijn omschrijft dat min of meer hetzelfde. Misschien dat in de kantine van de SBG spijzenen en dranken te krijgen zijn, maar dat maakt het geen zorginstelling. In de verste verte is de SBG niet tot een dergelijke instelling te rekenen. De rechters veegden dit dan ook van tafel.

Vonnis

De vaststelling van Btw-verplichting door de rechters betekent vooral ook dat “het SBG-gebeuren” en meer precies dus de samenwerking tussen de SBG en het ZN, als verzekeringskartel, door de rechter als zakelijke samenwerking/transactie tussen onafhankelijke ondernemingen is bestempeld, en dus niet als Btw-vrijgestelde zorgverlening, of zorgverlening gerelateerde service.

Raadsel

Het is mij een raadsel waarom de SBG, volledig betaald door ZN, deze actie tegen de belastingdienst in gang heeft gezet en waarom ZN in dit kader niet de SBG van deze beroepszaak afgehouden heeft.

In de het licht van de miljarden aan verzekeringsgeld die de zorgverzekeraars beheren en de in de afgelopen jaren gemaakte winsten is een verhoging van de betalingen van ZN aan de SBG om Btw-afdracht te faciliteren een peanut. Met krap twee ton op jaarbasis bovenop de huidige betaling aan de SBG had dit forse gezichtsverlies vermeden kunnen worden.

Het is zoals de Engelsen zeggen: “Penny-wise but pound-foolish”

W. J. Jongejan

Een kort geding over een grote kwestie

Het is en blijft een even lastige als netelige kwestie: gegevensverwerking in de zorg met behoud van vertrouwelijkheid en met respect voor het medisch beroepsgeheim. Zo lijkt in de kwestie die op 13 juli 2017 in kort geding werd voorgelegd aan de rechter vrijwel door iedereen, maar niet door de rechter, een essentieel punt over het hoofd te worden gezien! Dit betreft het feit dat de uitkomsten van zogenaamde ROM(Routine Outcome monitoring)-vragenlijsten – op individueel niveau – naar Stichting Benchmark GGZ (SBG) worden verzonden SAMEN met de (alles behalve) minimale dataset (MDS) met gedetailleerde medische en sociaal economische informatie op individueel

niveau. Dit is dezelfde MDS dataset die via de op computers van zorgverleners geïnstalleerde software eveneens automatisch en geruisloos vanuit patiëntdossiers naar het DBC-Informatie Systeem(DIS) wordt verzonden. Voor de ontvangst en verwerking van deze gegevens ontbreekt bij SBG, net als eerder is geconstateerd bij aanlevering aan het DIS, een wettelijke grondslag.

Kluisje

Zowel de minimale dataset als de uitkomsten van vragenlijsten worden bij SBG opgeslagen in een bestand dat zij de naam "kluisje" hebben gegeven. Deze gegevens liggen daar om later gebruikt te kunnen gaan worden voor "onderzoek". En het is volstrekt onduidelijk voor welk soort onderzoek ze zullen worden gebruikt, of welke partijen betrokken zullen worden bij dergelijke onderzoeksprojecten, en over welke gegevens/databestanden samenwerkingspartijen bij een onderzoek zullen of kunnen beschikken (denk bijv. aan projecten die worden gestart via het Inlichtingenbureau). De beslissing over het gebruik van de data in het "kluisje" (gebruik voor "onderzoek") ligt bij SBG.

Plank mis slaan

Omdat deze gegevens bij onderzoek worden gebruikt voor een ander doel – de Wet bescherming persoonsgegevens(Wbp) vereist dat dit doel welomschreven is – dan waarvoor zij oorspronkelijk verzameld zijn, stelt SBG dat daarvoor elke keer toestemming zal worden gevraagd aan de zorgverlener. En laat SBG hier de plank nu helemaal mis slaan, aangezien zij kennelijk niet beseft dat een dergelijke toestemming niet aan zorgverleners moet worden gevraagd maar daarentegen aan patiënten/cliënten.

En het wordt nog erger vanwege het feit dat SBG kennelijk ook niet beseft dat deze toestemming vrijelijk moet worden verkregen en niet onder druk van het niet-vergoeden van behandelingen (niet contracteren zorgverleners indien norm voor doorgifte m.b.t. ROM-gegevens niet wordt gehaald).

Of het nu gaat om de aanlevering van gegevens aan SBG, aan het DIS, aan gemeenten en “onze ministers” in het kader van de jeugdzorg, dan wel om de verwerking van medische persoonsgegevens door zorgverzekeraars op basis van verwerkingsprocedures waarvan de rechter heeft bepaald dat deze geen juiste uitwerking vormen van het Wbp, in al deze gevallen zien we dat bij de opzet van informatiesystemen in de zorg op z’n zachts gezegd onvoldoende aandacht is besteed aan de privacy van patiënten/cliënten, aan de privacy van burgers.

Afschaffing medisch beroepsgeheim
Zo wordt heel geleidelijk via aanpassingen van verschillende wetten, regelingen en procedures voor gegevensverwerking de vertrouwelijkheid van de spreekkamer volledig opgeheven. Met volle steun van onze overheid wordt stap voor stap en liefst zo geruisloos mogelijk (of onder de noemer van verbetering “cliëntenrechten”) het medisch beroepsgeheim afgeschaft. Om zonder de vereiste toestemming van patiënten het verwerken van medische gegevens door SBG te legitimeren heeft demissionair minister Schippers zich direct bereid verklaard om een “reparatiewetje” te maken om zo de toestemming van patiënten en het medisch beroepsgeheim te omzeilen door zorgverleners wettelijk te verplichten de verre van minimale MDS dataset “verrijkt” met informatie van ROM-vragenlijsten aan te leveren bij SBG.

Verdient het opheffen van vertrouwelijkheid en medisch beroepsgeheim in de zorg niet een serieus maatschappelijk debat en meer aandacht in de media? Is afschaffing van vertrouwelijkheid in de zorg nu echt wat we als burgers willen?

Mr. Ab van Eldijk voorzitter KDVP (Stichting de Koepel van DBC- vrije Praktijken van Psychotherapeuten en Psychiaters voor behoud van privacy, beroepsgeheim en zelfbeschikking)

Weer sloppy science vanuit Nijmeegs ReShape Center

Op 5 juli 2017 verscheen in de mhealth- en uhealth-editie van het Journal of Medical Internet Research een artikel genaamd: "Continuous Monitoring of Vital Signs Using Wearable Devices on the General Ward: Pilot Study". Het betrof een vergelijking van twee kleine apparaten, de Visi Mobile van Sotera Wireless en de Healthpatch van VitalConnect. Het onderzoek had als doel met deze apparaten vroegtijdig klinische verslechteringen in de gezondheidstoestand te ontdekken bij opgenomen patiënten. Bij lezing van het artikel valt op hoe ondanks allerlei forse onnauwkeurigheden en problemen blijmoedig het gebruik van deze apparatuur gepropageerd wordt als veelbelovend. Kwalitatief stelt dit onderzoek zelfs voor een pilot study weinig voor. Ik wees al eerder op een weinig voorstellende studie vanuit het ReShape Center. Het is zeker niet het eerste artikel vanuit het Radboud Universitair Medisch Centrum dat in voornoemd tijdschrift wordt gepubliceerd. Steevast staat de directeur van het ReShape Center van deze instelling, Lucien Engelen, als co-auteur vermeld. Weinig bekend is dat hij zelf lid is van de editorial board van de mhealth– en uhealth-editie van het JMIR. Het roept de verdenking op dat bij publicaties in dit blad een slager zijn eigen vlees keurt ook al wordt een aangeboden publicatie door een mede-editor behandeld, zoals vermeld onder het huidige artikel. Het ware verstandiger om

dit soort situaties te vermijden.

Vreemd

Heel apart is dat het onderzoek gedaan is tussen december 2014 en maart 2015 en dat de publicatie in juli 2017 plaats vindt. Een gat van ruim twee jaar zit er dus tussen. Voor iets wat veelbelovend is in een tijd waarin elektronische ontwikkelingen razend snel gaan is dat heel vreemd. Onder het artikel staat vermeld dat het pas eind 2016 ingediend is bij het JMIR.

Hoe wearable?

Terwijl de Healthpatch nog wel een kleine sensor genoemd kan worden die op de borstkas op de huid geplakt zit, is de Visimobile dat toch echt niet. Het apparaat dat de patiënt op de pols bevestigd krijgt weegt samen met een aan een kabel verbonden bloeddrukmodule om de bovenarm een kwart kilo. Een ademhalingssensor op de borstkas en drie ECG electroden hebben ook kabels lopen naar de polsmodule. Beide apparaten hebben via een wifiverbinding een basisstation nodig dat continu gemonitord moet worden. Bij de specificaties van de Visi Mobile is trouwens ook te zien dat de accu na 12 tot 24 uur leeg is en dan vervangen moet worden. Het bedrijf dat het apparaat maakt, Sotera Wireless, werd in 2016 failliet verklaard mede door een rechtszaak vanwege ongelicenceerd gebruik van andermans technologie. Na een nieuwe kapitaalinjectie van 30 miljoen euro zette het de activiteiten weer voort.

Opvallend

In de studie werden de metingen van de twee apparaten met de metingen door de verpleging vergeleken. Het gaat om de meting van bloeddruk, hartfrequentie, ademhalingsfrequentie, zuurstofsaturatie en (kern)lichaamstemperatuur. Direct opvallend is dat beide onderzochte apparaten niet dezelfde functionaliteit hebben. Zo meet de Healthpatch geen bloeddruk.

Beide apparaten meten de huid-, maar niet de kerntemperatuur van de patiënt. Bijzonder opvallend is het geringe aantal mensen in de studie, namelijk 20. De facto zijn slechts de gegevens van 12 patiënten gebruikt omdat tijdens de studie op onverklaarbare wijze de naar een laptop doorgeseinde data van 8 patiënten verloren gingen. Van de 120 metingen(verpleegkundigen versus appraten) die men wilde vergelijken vielen er 34 af. Aan de kant van de verpleegkundigen waren 9 meetclusters onvolledig, aan de apparatenkant 25. 86 meetclusters van 12 patiënten zijn dus gebruikt. Gemiddeld iets meer dan 7 per patiënt. Dat is bitter weinig als je een studie doet over het monitoren van patiënten.

Spreiding

Bij het zien van de Bland-Altman-plots van de gemeten data valt op dat er forse verschillen en uitschieters waren van de meetwaarden met de apparaten vergeleken met die van de verpleegkundigen. Ook in de plots van de Modified Early Warning Scores was er een grote spreiding, dus beperkte conformiteit met MEWS-scores van de verpleegkundigen.

Artefacten

De metingen van de Visi Mobile en de Healthpatch werden continu gemonitord door daarvoor getrainde medische studenten. Zij zagen bij de Visi Mobile 306 artefacten(lees: (ver)storingen) in de registratie gedurende 121 uur. Bij de Healthpatch 648 in 135 uur. Dat zijn respectabele aantallen. Het kon variëren van verlies van huidcontact van de elektroden tot problemen met de laptop waarop de data opgeslagen en beoordeeld werden. Ze duurden van 5 minuten tot een uur. Voor het geringe aantal patiënten en het aantal beoordeelbare meetwaarden is het aantal artefacten bijzonder groot te noemen. Indien er geen medisch student de overdracht of opslag van data gevolgd had, zouden de verpleegkundigen zeer frequent geen signaal ontvangen hebben of zeer frequent op een

registratiealarm hebben moeten reageren.

Ongefundeeerd techno-optimisme

Ondanks alle problemen komen de schrijvers toch tot de nogal optimistische conclusie dat de Visi Mobile en de Healthpatch veelbelovende apparaten zijn die goed ontvangen werden door patiënten en verpleegkundigen. Bij de conclusies noemt men als eerste het gevoel van geruststelling van de patiënt en verwanten dat deze gemonitord wordt. Dat is nu niet bepaald een wetenschappelijk argument om iets wel of niet toe te passen. De vraag moet zijn of het medisch noodzakelijk is dergelijke apparatuur te gebruiken om gezondheidswinst te bereiken of tenminste gelijkwaardige zorg tegen lagere kosten/moeite te leveren. Als tweede noemt de mogelijke vroegere waarschuwing van verslechtering van functies bij drie patiënten.

Nieuwe proef

Ondanks deze bevindingen gaat het Radboud UMC zonder de naam van de Visi Mobile te noemen binnenkort een proef nemen met alle 60 opgenomen patiënten op de afdeling interne geneeskunde en chirurgie. Aangezien een kastje om de pols gebruikt wordt moet het wel dat apparaat zijn. Eigenlijk wordt op deze wijze een hele afdeling tot een soort hartbewakingseenheid omgetoverd. Blijkens het persbericht houdt een computerprogramma de binnenkomende waarden in de gaten. Ik mag toch hopen dat verpleegkundigen en artsen op de afdelingspost de binnenkomende waarden ook in het oog houden. Alleen al daardoor en door het veelvuldig voorkomen van artefacten, wat bij de uitgebreide bekabeling niet verbazingwekkend is, plus het binnen een dag moeten vervangen van accu's betekent dat een forse verzwaring van de taken van verpleegkundigen op de afdeling. Het lijkt me dan ook een logistieke nachtmerrie.

W.J. Jongejan

Kwaliteitsinstituut van/voor GGZ: oude wijn in nieuwe zakken

Twee dagen voor het kort geding op 13 juli van de actiegroep StopBenchmarkROM versus de Stichting BenchmarkGGZ verscheen op 11 juli plotseling op de website van Zorgverzekeraars Nederland(ZN) een persbericht. Hierin de mededeling dat doorontwikkeling van ROM-verwerking gaat plaatsvinden binnen een nieuw op te richten kwaliteitsinstituut voor de Geestelijke GezondheidsZorg(GGZ). De Routine Outcome Monitoring(ROM) doet sinds januari 2017 erg veel stof opwaaien. Bij reeds bestaande kritiek vanuit de GGZ dat ROM-data niet geschikt zijn voor benchmarking en zorginkoop liet de Algemene Rekenkamer toen weten dat dat ROM-data absoluut ongeschikt zijn om gebruikt te worden daarvoor, en zeker niet in het kader van de bekostiging van de GGZ. De ROM-data zijn tot voor kort stelselmatig verzameld en verwerkt door de SBG. Deze instelling, die volledig gefinancierd wordt door de zorgverzekeraars(lees ZN), heeft de afgelopen twee jaar niet anders beweerd dan het (willen) door-ontwikkelen van de ROM-data om de data meer zeggingskracht te geven. Men heeft daar

ook wel door dat de ROM-data niet ideaal zijn voor het doel waarvoor de SBG is opgericht, maar blijft er toch aan vasthouden. Het fundamenteel onjuiste van het gebruik van ROM-data voor benchmarking en zorgkoop is gelegen in het doel waarvoor ROM ooit ontwikkeld is, namelijk het evalueren en bijsturen van individuele therapie. Het gebruik op geaggregeerd niveau is een nooit bedoelde, niet valide en dus onjuiste toepassing.

Kort geding

In de aanloop naar het kort geding bleek meerdere keren dat SBG en op de achtergrond ZN de wederpartij kleine brokjes toewierpen. Zo verscheen tien dagen voor het geding plotseling de melding op de website van SBG dat in de Minimale DataSet nu expliciet staat dat postcode en land van herkomst van de patiënt versleuteld worden en geaggregeerd worden aangeleverd aan de SBG. Iets waar voordien nooit duidelijk was. Beide items zijn van belang in het kader van de herleidbaarheid van informatie naar een individu. Diezelfde dag liet de SBG opeens weten dat enkele cijferreeksen in de ROM-data, het zorgtrajectnummer, het DBC-trajectnummer en het koppelnummer, sinds kort gepseudonimiseerd en later gerandomiseerd worden. Het zijn ook data die kunnen leiden tot het terugvinden van een individu in de aangeleverde databrij. Ook had men een begin gemaakt met het met terugwerkende kracht uitvoeren van deze bewerking op reeds aangeleverde data. De acties van de SBG passen in de tactiek van het eerst negeren, dan traineren en vervolgens piece-meals-gewijs toestoppen van zaken die de tegenstander mogelijk zou kunnen bewegen het kort geding niet door te laten gaan.

Oude wijn

Met veel omhaal van woorden, waarbij men zorgvuldig de woorden benchmarking en zorginkoop vermijdt, is nu het buzzwoord “kwaliteit”. Men vergeet daarbij dat Routine Outcome Monitoring alleen valide is in de individuele relatie tussen

patiënt en therapeut om de therapie bij te sturen, maar dat het instrument niet geschikt is om op geaggregeerd niveau “kwaliteit” te meten om daarmee “transparantie” te bieden aan professionals en patiënt. Ondanks alle mooie woorden gaat het onder de streep bij de zorgverzekeraars toch om het afrekenen van zorgaanbieders op basis van die “gemeten kwaliteit” en blijft het dus oude wijn in nieuwe zakken. In de somatische zorg is de laatste twee jaar heel langzaam het inzicht gegroeid dat met aangeleverd cijfermateriaal(indicatoren) van zorgaanbieders niet altijd één op één kwaliteit te meten is. ZN en de SBG weten dat de ROM-data een wankele basis voor hun doel zijn, want al tijden en nu ook weer spreekt met over het doorontwikkelen van de ROM-systematiek. Het is eigenlijk het proberen om een slecht gebouwd vehikel al rijdend af te bouwen tot iets wat op een auto lijkt.

Kwaliteitsinstituut=SBG

In het hele persbericht spreekt ZN met geen woord over de SBG, waar tot nu toe alle ROM-verwerking plaats vond. Het is dan ook overduidelijk dat het nieuw te maken kwaliteitsinstituut niets anders is dan een voortzetting van de huidige SBG, maar dan onder een andere naam. Tijdens het kort geding zei de advocaat van de SBG rond 10.30 uur ook dat de SBG een belangrijke rol zal spelen bij het doorontwikkelen van ROM zoals onlangs door de partijen is afgesproken. Duidelijker kan het niet.

Doortrapt

De naamgeving van de voortzetting van de SBG onder andere vlag is doortrapt gekozen. Benchmarking en zorginkoop is iets wat direct geassocieerd wordt met de achterliggende broodheer van de SBG, namelijk ZN. De naam kwaliteitsinstituut lijkt te appelleren aan iets anders, maar is het au fond niet. Publicitair gezien is het makkelijker tegen benchmarking of zorginkoop te zijn dan tegen kwaliteit.

Brede consensus??

Onder het persbericht staan organisaties vermeld van de koepel van werkgevers in de GGZ, koepels van behandelaars en een patiëntenorganisatie. Dat lijkt heel aardig maar al deze partijen deden al mee aan SBG en waren de afgelopen jaren door een convergerend afsprakenstelsel van massage met financiële middelen(waaronder ook financiële korting op betalingen voor geleverde zorg bij niet aanleveren van ROM-data) zover gebracht dat ze meededen aan de ROM-data-levering.

Essentie

ZN spreekt over doorontwikkeling van ROM. Daar gaat het echter niet over. Het gaat om het doorontwikkelen van instrumenten voor benchmarking en zorginkoop op basis van ROM-data. De **essentie** waarom men doorgaat wordt door ZN in de eerste alinea meer dan duidelijk verwoord: **“De afgelopen jaren is veel tijd en geld geïnvesteerd in ROM”.** Het is het aloude verhaal van een wrakke olietanker die in de vaart is gebracht en niet uit de vaart genomen wordt en al varende telkens wat van koers verandert.”

De slotconclusie bij het persbericht van ZN kan niet anders zijn dan dat het oude wijn in nieuwe zakken is.

W.J. Jongejan

Hackers bieden Australische

Medicare-card-data te koop aan. Les voor Nederland

Op 4 juli 2017 werd duidelijk dat op het zogenaamde Dark Web, een alleen met een speciale browser toegankelijk deel van het internet, gegevens te koop waren van Australische Medicare-ID-kaarten. Dat zijn kaarten met een magneetstrip, die de bezitter toegang geeft tot behandeling in de eerstelijnszorg en zorg in publieke ziekenhuizen. De melding kwam van een journalist van The Guardian, die op het Dark Web voor 22 US dollar, of 0,0089 bitcoin, de data van zijn eigen medicare-card kocht. Degene die de data verkocht had sinds oktober 2016 data van tenminste 75 Medicare-kaarten verkocht. De kaarten worden uitgegeven door het Australische Department of Human Services. De details van de kaarten, zoals nummer, tenaamstelling en expiratiedatum zijn niet publiek toegankelijk en zijn alleen de eigenaar van de kaart bekend. Door criminelen wordt de informatie als waardevol beschouwd. omdat ze het mogelijk maken om nep-Medicare-kaarten te maken met bestaande gegevens. Die kunnen dan gebruikt worden voor identiteitsfraude.

Waardevol

Al enige tijd is het duidelijk dat diefstal van medische gegevens veel lucratiever is dan het bemachtigen van creditcardnummers. Cybersecurity-adviseurs denken dat medische gegevens, inclusief de polis- en persoonsnummers(social-security-numbers of BSN) tot tien keer meer waard zijn dan

creditcarddata. De gegevens op de kaarten kunnen gebruikt worden door criminelen voor de aanschaf van goederen, bijv. auto's. Ook kunnen uitbetalingen van Medicare aan de burger doorgesluisd worden naar frauduleuze bankrekeningen. Al in 2015 had een politie-eenheid een criminele groep opgespoord die Medcare-card data gebruikte om zich frauduleus terugbetalingen toe te eigenen. Een probleem in Australië is tevens dat de Medicare-card ook als identificatiemiddel(Digital Verification Service) buiten de zorg wordt gebruikt. Dat bleek toen de Australische belastingdienst, de Australian Tax Office met onmiddellijke ingang aangaf dat de Medicare-card niet meer gebruikt mocht worden als identiteitsverificatie bij belastingzaken. Het vreemde was dat nog geen 24 uur later dezelfde dienst aangaf dat de kaart weer als identificatiemiddel mocht worden gebruikt.

Overheid

Zoals te verwachten probeerde de overheid bij monde van de minister van het Department of Health Services direct het belang te downplayen onder andere dat het ging om kleine aantallen. De stelling van minister Tudge is dat het hier niet om een hack ging maar om een "traditional criminal activity" gaat en niet om een groot datalek. De minister bleek tot aan 5 juli 2017 niets van de diefstal van card-data te weten ook al waren de data al vanaf oktober 2016 te koop op het Dark Web. De berichtgeving via de pers schudde het ministerie wakker.

Medische data

Naar verluidt zijn bij de diefstal van de kaartdata niet rechtstreeks medische data in handen van criminelen gekomen. Wel zijn bij de diefstal de koppeling van naam en Medicare-nummer van de betrokkenen buitgemaakt. Om bij de medische data te komen zijn elektronische NASH en/of PKI-certificaten nodig. Die worden echter door de overheid naar duizenden zorgverleners verstuurd en naar verluidt zijn daarvan meerdere

“zoekgeraakt”. Misbruik is dus niet uit te sluiten.

Medicare

Het gecentraliseerde Medicare-ysteem stond en staat bloot aan veel kritiek en is toch doorgeduwd. Medische data worden in een centrale database opgeslagen. In noodgevallen mogen artsen de medische gegevens van burgers in “My Health Record” zonder toestemming van de patiënt inzien. De overheid mag de medische data zonder toestemming inzien als fraude vermoed wordt of bij rechtszaken. Medicare gaat ook onzorgvuldig om met data. Recent werden deels versleutelde databestanden openbaar beschikbaar gesteld die door enkele academici binnen korte tijd vergaand te ontcijferen waren. De vreemde reactie van de overheid was toen om het ontcijferen strafbaar te stellen in plaats van het te accepteren als een waarschuwing!!!

Nederland

Wat leert deze materie ons Nederlanders? Wij hebben ook een gecentraliseerd systeem met het Landelijk SchakelPunt(LSP). De data zijn niet centraal opgeslagen, maar zijn bij de bron raadpleegbaar via het LSP. De toegang is geregeld met UZI-passen en kaartlezers. Diefstal van UZI-pas en pincode van de gebruiker maakt het in principe mogelijk dat door die dief vanaf een werkstation plus kaartlezer met malafide intenties ingelogd kan worden en data opgevraagd worden. Uiteraard vindt logging plaats van het gebeurde en is de toegangsweg te identificeren, maar het kwaad is dan al geschiedt zonder dat men weet wie de dader is. Men weet alleen wiens pas gebruikt is en mogelijk welke werkplek. Bovendien zal het de gedupeerde burger niet altijd duidelijk zijn dat zijn of haar data ingezien zijn als deze geen abonnement heeft op meldingen van inzage in de medische gegevens via het LSP.

Kortom: het kan ook hier gebeuren, het is alleen de vraag wanneer en hoe uitgebreid.

W.J. Jongejan

Centraal PlanBureau op zeer glad ijs met advies tot verplichting LSP

Op 3 juli 2017 publiceerde het Centraal PlanBureau(CPB) een notitie, genaamd Risicorapportage Cyberveiligheid Economie. Cyberveiligheid is een hot issue, zeker na de recente Petya-ransomware-cyberaanval. Wereldwijd, ook in Nederland werden bedrijven, maar ook overheidsinstellingen daardoor tijdelijk uitgeschakeld. Het CPB gaat uitgebreid in op de economische gevolgen van het falen van ICT-systemen door cyberaanvallen. In haar notitie neemt het CPB ook de zorg mee. De argumentatie daarvoor is dat de zorgsector niet alleen primair van belang is voor de gezondheid van de bevolking maar dat ook het economische belang substantieel is. De uitgaven aan de gezondheidszorg zijn verantwoordelijk voor veertien procent van het bruto binnenlands product. Bovendien draagt in de woorden van het CPB een gezonde (beroeps-)bevolking bij aan welvaart en welzijn. In haar adviezen om problemen te voorkomen komt het CPB met een aantal opmerkelijke uitspraken, onder andere door te stellen dat de overheid kan overwegen om poortwachters en zorgverleners te verplichten om via een

veilige publieke infrastructuur gegevens uit te wisselen. Ze noemt dan met name het Landelijk SchakelPunt(LSP).In de redenatie van het CPB zitten een aantal ongerijmdheden en lijkt zij niet goed op de hoogte te zijn van de realiteit rond het LSP.

Geen kennis van zaken

In de notitie van het CPB staat dat 91 procent van de huisartsen aangesloten is op het LSP en dat het gebruik lager lijkt te liggen. 68 procent van de huisartsen lijkt het LSP slechts te gebruiken. Wat niet vermeld wordt, maar al lange tijd speelt, is dat de Nederlandse burger maar zeer beperkt bereid is de gegevens die bij de huisarts opgeslagen zijn te delen via het LSP. Op de website van VZVZ is heden 8 juli te zien dat slechts 6,1 de 17,1 miljoen Nederlanders dat wil. Dat is dus maar 35 %. Daarbij moet nog aangetekend worden dat niet alle toestemmingen legitiem verkregen zijn. Bij dit alles vergeet het CPB ook dat zelfs als alle zorgaanbieders op het LSP aangesloten zijn, burgers geen verplichting hebben om toestemming te geven om hun medische gegevens te doen delen. Het CPB blijkt geen benul te hebben van de systematiek van het LSP. Het is in wezen een legacy-systeem met een verouderde centrale opzet waarin een centrale verwijsindex de belangrijkste rol speelt. In die verwijsindex zijn de opgevraagde data kortdurend onversleuteld aanwezig, wat niet meer van deze tijd is. Dat wordt door professor Eric Verheul, hoogleraar bij de Digital Security Group van de Radboud Universiteit van Nijmegen, uitermate helder bekritiseerd. Hij stelde in zijn betoog tijdens een hoorzitting in de Eerste Kamer op 29 april 2016, dat de opzet van het LSP thans volledig achterhaald is.

Aparte aanname

Het CPB komt tot aparte aanname. In hoofdstuk 4.2 onder de alineakop Verzekeraars zegt het bijvoorbeeld:

“Vektis en verzekeraars beschikken over administratieve gegevens waaruit de gezondheid van iedere Nederlander af te leiden valt. Risico’s op datalekken en onvoldoende beveiliging lijken op dit moment echter beperkt omdat verzekeraars baat hebben bij een goede reputatie. Verzekeringsnemers kunnen immers naar een andere verzekeraar overstappen als zij hun huidige verzekeraar niet vertrouwen – al is de keuze uit zorgverzekeraars beperkt.”

Deze aanname is typisch een geval van natte-vingers-werk. Dezelfde redenatie is op te hangen over zorgaanbieders, zoals bijv. huisartsen. Die hebben ook baat bij een goede reputatie. Patiënten kunnen bij gebleken datalekken ook van zorgverlener gaan veranderen. Ook de gedachte dat het goed zou zijn een publieke infrastructuur verplicht te stellen is vreemd.

Zeer tegenstrijdig

Het CPB pleit er dus voor dat zorgverleners de informatie uitsluitend delen via één veilige publieke infrastructuur, daarbij expliciet het LSP noemend, door het gebruik verplicht te stellen. Een verplichte publieke infrastructuur voor gegevensuitwisseling in de zorgsector kan volgens het CPB naleving van normen makkelijker maken, voorkomt volgens hen afhankelijkheid van een enkele private partij en kan burgers inzicht geven in wie toegang tot hun gegevens heeft. Het CPB stelt dat onderzocht kan worden of deze voordelen opwegen tegen de risico’s. Men zegt ze dat er twee risico’s verbonden zijn aan het gebruik van een publieke infrastructuur. Het eerste risico is dat er bij het wegvallen van zo’n infrastructuur grootschalige problemen kunnen ontstaan. Dat is het risico op een “single point of failure”. Vervolgens komt men met een oplossing daarvoor door te zeggen dat een dergelijk risico beperkt kan worden door pluriformiteit en decentraal te organiseren, bijvoorbeeld met blockchain-technologie. Na eerst een centraal systeem te adviseren komt het CPB nu opeens een decentrale gedachte op de proppen met de suggestie van het gebruik van een technologie, blockchain, die

in de zorg en elders als veelbelovend (Nictiz, januari 2017) wordt beschouwd maar niet rijp is voor brede toepassing op dit moment. Bovendien vond in 2016 er een opmerkelijke blockchain hack plaats, de DAO-hack. Het Nictiz zegt daarover dat deze hack heeft laten zien dat het onwijzigbare karakter van de blockchain niet alleen maar voordelen heeft.

Ander risico

Het CPB noemt als tweede risico van een centrale publieke infrastructuur dat als deze niet gebruiksvriendelijk ontworpen is zorgverleners gebruik gaan maken van onveilige alternatieven. Men adviseert dan ook te investeren in gebruiksgemak. Het LSP kent duidelijke beperkingen in het functioneren. In dit kader wil ik wijzen op een eerder publicatie van mij op 26 mei 2017, waarin ik dit aankaart en wijs op ongewenste workarounds door gebruikers.

Zorgvisie

Het online magazine Zorgvisie maakte het met de bekendmaking van de CPB-notitie helemaal bont door te reageren met een artikel met als kop: “LSP als wapen tegen cybercriminelen”. Het geeft aan dat men daar niet goed begrijpt dat wat het CPB zegt een defensieve gedachte is en niet een offensief wapen tegen cybercriminelen.

Onterechte stellingname CBS

Een adviesorgaan van het ministerie van Economische Zaken, hoort geen uitspraak te doen over het verplicht stellen van deelname aan het LSP. Het is de minister van VWS in 2011 bij het wegstemmen in de Eerste Kamer van het publieke Landelijk Elektronisch Patiëntdossier uitgebreid te verstaan gegeven geen financiële of organisatorische bemoeienis meer te hebben met het LSP. Het CPB moet, niet volledig op de hoogte zijnde van het functioneren van het LSP, dit als onderdeel van EZ dan niet toch te gaan doen.

W.J. Jongejan