Veelvuldige (85x) onrechtmatige inzage dossier Barbie noodt tot notificatieplicht

Begin april 2018 bleek dat bij de opname van de "reality tv-ster"Samantha de Jong alias Barbie in het Haga-Ziekenhuis in Den Haag begin dit jaar meerdere personen onrechtmatig het elektronische medische dossier inkeken. Vijfentachtig bleken het te zijn. Die komen er allemaal met een waarschuwing van af. Het gaat om mensen, die geen medische behandelrelatie hadden met deze patiënt. Er is dan naast het onfatsoenlijk handelen sprake van het overtreden van gedragsregels, het privacyreglement van het ziekenhuis en de beroepsnormen die voor diverse soorten werkers gelden. Ik doel in dat kader op artsen en verpleegkundigen. De overtredingen in het Haga-Ziekenhuis kwamen naar buiten na het opvragen van logging-gegevens van het ZiekenhuisInformatieSysteem(ZIS). Ondanks eerdere incidenten en waarschuwingen van de Autoriteit Persoonsgegevens heeft dit zeer grootschalige incident kunnen plaatsvinden. Het is mijns inziend derhalve noodzakelijk om naast passende maatregelen voor de toegang tot de dossiers ook een notificatieplicht in te voeren richting patiënt en wel direct bij elke inzage in het dossier.

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens(AP) heeft in 2016 klip en klaar aan Raden van Bestuur van alle zorginstellingen een waarschuwing doen uitgaan om dit soort incidenten door passende maatregelen in de elektronische dossiervoering de wereld uit te helpen. Als de zorginstellingen waarvoor de bestuurders verantwoordelijk zijn voornoemde zaken niet goed geregeld hebben, is er sprake van een overtreding van artikel 13 van de Wet bescherming persoonsgegevens. Blijkbaar heeft het Haga-Ziekenhuis niet afdoende maatregelen genomen om de onrechtmatige inzage te voorkomen en is daardoor mede verantwoordelijk voor het gebeuren..

Maatregelen

De maatregelen om inzage te voorkomen zijn soms boterzacht. In sommige ziekenhuizen kan men een zogenaamde VIP-status krijgen. In het dagblad Trouw staat dat sommige ziekenhuizen in zo'n geval een extra scherm doen zien bij poging tot inzage van het medisch dossier met een waarschuwing dat er wel een behandelrelatie moet zijn. Ik mag hopen dat ze daarnaast de patiënt in zo'n geval ook met een fictieve naam inschrijven.

Notificatieplicht

Het aanvragen van een VIP-status moet niet nodig zijn, want bij elke patiënt kan er wel iets zijn waar iemand om wat voor reden in geïnteresseerd kan zijn. Jurisprudentie daarover laat dat ook zien. Veel duidelijker en afschrikwekkender is het als er een momentane notificatieplicht komt voor zorginstellingen. Daarbij doel ik op het melden van iedere inzage in het dossier aan de patiënt op het moment dat die inzage plaatsvindt, gekoppeld aan de logging in het ZIS. Dat is op velerlei wijze te realiseren. Het kan uitgevoerd worden middels berichtgeving via het ziekenhuisportaal, waarmee de patiënt nu al vaak met het ziekenhuis elektronisch kan communiceren(afspraken, medicatie, inzage dossier) bijv. op de smartphone of op de PC. Daarbij kan het zo ingesteld worden dat voor de patiënt herkenbaar bij de behandeling betrokkenen na goedkeuring

uitgesloten kunnen worden. Het is bijv. door een simpele vraag aan de patiënt daarover en vastlegging in het ZIS te realiseren. De hoeveelheid notificaties kan zo beperkt worden. Eventueel kan bij opname gevraagd worden aan de patiënt en zijn naasten of men wel prijs stelt op deze dienstverlening.

Afschrikwekkend

Naar mijn oordeel is een notificatieplicht meer afschrikwekkend dan allerlei gedragsregels, pop-up-schermen enzovoort. Iedere potentiële overtreder kan na invoering van een notificatieplicht weten dat real-time de patiënt in kennis wordt gesteld van die inzage. Het voorkomt ook een ander probleem. Dat is de onwil van sommige zorginstellingen om op aanvraag rap en zonder tegenstribbelend commentaar log-gegevens beschikbaar te stellen. Ook het tegenstribbelen ten aanzien van het aangeven bij de AP van een datalek indien onbevoegde inzage plaatsvond, is dan meteen uit de wereld.

Opportunistisch

Aannemende dat werknemers van het Haga-Ziekenhuis hadden kunnen weten dat onbevoegd inzien van medische gegevens norm overschrijdend is, is het geven van een waarschuwing aan de 85 overtreders nogal opportunistisch. Jurisprudentie laat zien dat ontslag zeer wel mogelijk is in dergelijke gevallen. Het ziekenhuis zou dan wel een probleem hebben met de personeelsbezetting!

Tuchtraad

Wel is het mogelijk dat verpleegkundigen en artsen op persoonlijke titel voor de tuchtrechter kunnen worden gebracht, hetzij door het bestuur van het ziekenhuis hetzij door de patiënt. Ook de Inspectie Gezondheidszorg en Jeugd(IGJ) zou dit kunnen doen om het maatschappelijk belang van het schenden van beroepsnormen in dezen voor de twee beroepsgroepen te onderstrepen.

W.J. Jongejan, 27 april 2018

Orangeworm (hackersgroep) bedreigt medische software o.a. van scanners

Sinds kort is de hackersgroep Orangeworm zeer actief om met het Kwampir-virus netwerken te besemetten. Men heeft het daarbij speciaal gemunt op de medische sector, omdat veertig procent van de besmettingen gevonden is in computersystemen van ziekenhuizen, medische apparatuur en toeleveringsbedrijven van zorginstellingen, maar ook farmaceutische bedrijven. Het Kwampir-virus, waarmee deze hackersgroep, waarvan eigenlijk nauwelijks iets bekend is, behoort tot de categorie van de Trojan-horse virussen en wordt meestal als Win32/Kwampir aangeduid. Het lijkt erop dat Organgeworm niet willekeurig te werk gaat, maar gericht zijn doelen uitzoekt om te besmetten.

Het virus is al in 2015 ontdekt. Symantec, één van de grote bedrijven die antivirus-software maakt, beschreef in 2016 al wat dit virus doet en hoe het verwijderd moet worden. Het virus creëert binnen de besmette hardware een zogenaamde “backdoor”, waardoor het toegang heeft tot een besmet systeem en ook bestanden kan downloaden.

Beeldvormende systemen

Binnen ziekenhuizen is het virus ook aangetroffen op beeldvormende systemen(Medical Imaging Devices), zoals Röntgenapparatuur en MRI-scanners. Het binnendringen van virussen in de besturingssystemen van beeldvormende systemen is een groot probleem. Virussen kunnen de werking van die apparaten verstoren en schade berokkenen aan de patiënten en de apparatuur. Ik schreef er zeer kort geleden een artikel over. Het binnendringen van computervirussen in ziekenhuizen is sowieso een groot probleem, omdat hele systemen plat gelegd kunnen worden, maar ook gevoelige data de zorginstellingen onrechtmatig kunnen verlaten. Met het virus lijkt de hackersgroep ook gefocust te zijn op onderdelen van ziekenhuissoftware, waarin de patiënt toestemmingen vastlegt voor een noodzakelijke behandeling(en). Dat is ook een zeer zorgelijke ontwikkeling omdat op die wijze onterechte en onrechtmatige toestemmingen van patiënten in de ziekenhuissystemen terecht kunnen komen.

Werking

Het virus lijkt niet al te geheim zijn werk te doen en is op zich niet moeilijk te detecteren. De malware kopieert zich in onderdelen van een ICT-netwerk en verspreidt zich via een bepaalde lijst van “command and control” computerservers. Het cybersecurity-bedrijf Symantec denkt dat het de bedoeling is dat Orangeworm ten dele bedoeld is om de infrastructuur van aangetaste systemen vast te leggen, maar dat een aanval nog kan komen. Die aanval kan dan gebruik maken van de verzamelde data over de systemen. Symantec heeft ook een lijst van

zogenaamde Indicators of Compromis(IOC). (bron Webwereld) Daarmee kunnen systeembeheerders aan de hand van zogenaamde “fingerprints” zoeken naar kenmerken van het virus binnen de instellingssoftware.

Daders

Op dit moment gist men noch wie er achter de doelgerichte aanvallen zit met een relatief “oud” virus, dat ook relatief makkelijk te detecteren is. Binnen de cybersecurity-wereld denk men eerder aan een individu of een kleine groep individuen dan aan een door een staat georganiseerde of daardoor gefaciliteerde groep.

Zorgelijk

Het is uitermate zorgelijk dat zorginstellingen zo onder vuur liggen door criminele activiteiten. Anders kan je dit niet noemen. Het eventueel plat kunnen leggen van de systemen met ransomnware (zie Wannacry-virus-aanval) op basis van de vergaarde kennis met het Kwampir-virus is mogelijk. Daarnaast kan de werking van apparatuur geblokkeerd en verstoord worden. Ook kan na weglekken van administratieve en medische gegevens daarmee grootscheepse financiële fraude worden gepleegd. Op basis van gemanipuleerde toestemmingen voor behandelingen kunnen medische activiteiten bij een patiënt gestart worden die helemaal niet de bedoeling zijn.

Wake-up-call

Het is duidelijke wake-up-call voor werkers in de zorg en voor ICT-specialisten van zorginstellingen om alert te zijn op handelingen die de introductie van het virus mogelijk maken. Daarmee doel ik bijvoorbeeld op het gebruik van mobiele gegevensdragers zoals USB-sticks en mobiele harde schijven. Maar ook dient men consequent besturingssystemen te updaten met de laatste “patches” en erop toe te zie dat er geen door Microsoft of andere bedrijven uit gefaseerde besturingssystemen meer gebruikt worden.

W.J. Jongejan, 25 april 2018

Groot, traag, duur en vol lucht en VZVZ pimpt het op: het LSP(deel 2)

Dat valt tussen de regels door te lezen in het rapport over het Landelijk SchakelPunt (LSP) dat de Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ) op 19 april 2018 op haar website zette. Het heet "Rapport effecten en baten gebruik zorginfrastructuur". Gisteren besprak ik de eerste helft van dit rapport. Vandaag het tweede deel. Daarin een bespreking van de rest van de grafieken en tabellen die de "groei" van het LSP-gebruik aantonen, maar waar veel gebakken lucht in zit.

Opvragingen

VZVZ besteedt in het rapport veel tijd aan het aantal opvragingen van medicatie- of medische gegevens via het LSP. Er is een stijgende lijn te zien, maar wat onverbiddelijk terugkomt in de grafieken op pagina 18 onder hoofdstuk 5.6 is dat een groot aantal opvragingen niet succesvol is. Dat heeft

vooral te maken met het doen van opvragingen door zorgaanbieders ongeacht of de betrokken patiënt een opt-in-toestemming heeft gegeven. Dat kan namelijk technisch gewoon. Ondanks dat ik nimmer een opt-in-toestemmingen gaf, zijn er bij mij toch bijna 20 bevragingen door apotheken geweest. Die zijn dan allemaal niet succesvol. Zo zal altijd het aantal succesvolle bevragingen flink achterlopen bij het totale aantal bevragingen.

Gebakken ziekenhuislucht

VZVZ heeft lange tijd op haar eigen webpagina verkondigd(reeds in 2016) dat 89 % van de ziekenhuizen aangesloten was op het LSP. In de tabel op pagina 19, hoofdstuk 5.7 is te zien dat 78 van de 311 als ziekenhuis te beschouwen zorginstellingen eind 2017 aangesloten zijn op het LSP. **Dat is 25 procent.** Ook komt daarmee naar voren dat meerdere ziekenhuisinformatiesystemen nog geen LSP-module hebben ingebouwd. Jarenlang loog VZVZ dus de goegemeente voor.

Ketenbeschikbaarheid

In dit item op pagina 20, hoofdstuk 5.8, laat VZVZ zien in hoeverre bij het raadplegen van patiëntgegevens een technische verstoring optreedt. Ze komt dan tot een beschikbaarheid van 98,5%. Heel mooi, ben je geneigd te zeggen, maar VZVZ kijkt daarbij niet naar lokale verstoringen. Die zijn naar haar zeggen niet te meten, maar zijn er wel degelijk. Aangezien lokale systemen ook in de optiek van VZVZ een onlosmakelijk deel van de keten zijn zegt dit percentage dus helemaal niets. Immers de keten bestaat uit lokale systemen(goed beheerde systemen)- goed beheerde netwerken-LSP-goed beheerd netwerk-lokale systemen.

Weglaten nadere duiding

Op pagina 21 onder hoofdstuk 5.9 staan gegevens over de aantal bezoekers van het VZVZ-portaal waarop de inzage en toestemmingsverlening door de burger te checken is. Er staat

een piek na 21 maart 2017 als gevolg van de tv-uitzending van Zorg.Nu. VZVZ boekt dit hier heel sluw als belangstelling, maar de essentie van de piek lag hem in het feit dat in de uitzending de controle door de burger van een al dan niet terechte opt-in-toestemming ter sprake kwam. Velen, waaronder ik zelf, ontdekten dat men dat met name apothekers ten onrechte zo maar opt-in-toestemmingen noteerden. De drukte op de website was zo hoog dat de website bijna een dag plat lag.

Dure business

VZVZ komt in de tabel "Kosten in relatie tot volume gebruik" op pagina 21 onder hoofdstuk 5.10 tot een prijs van 11 eurocent per bericht in 2017. **Met een volume van 314 miljard berichten(voor een flink deel niet succesvol. Zie hierboven) telt dat op tot een bedrag van 34,6 miljoen euro in 2017.** Dat komt neer op 2 euro per Nederlander dat de zorgverzekeraars moeten betalen, terwijl een aanzienlijk deel van de burgers niet meedoet met belangrijke onderdelen van het LSP. Dit zijn dan de operationele kosten en bevatten geen ingrediënten bevatten die te maken hebben met investeringen in het systeem en het in stand houden van de infrastructuur. Die komen er nog bovenop.

Zeer duidelijke minpunten

Dat alles allemaal niet zo lekker loopt is te lezen in hoofdstuk 7 Verbetermogelijkheden. Daar lees je dat van de wel op het LSP aangesloten huisartsen 58 % het LSP niet gebruikt. Zij die het wel doen gebruiken in 17% de opgevraagde data nooit en 58 % soms.

Huisartsenposten laten weten, volgens het VZVZ -rapport, dat bij grote drukte het moeten ophalen van de Professionele Samenvatting(met medische gegevens bij de eigen huisarts) lastig is. **Dan is het gebruik van het LSP niet per se een oplossing, eerder een belemmering bij het doorwerken.** Apothekers melden het veelvuldig voorkomen van storingen en

daarnaast foutmeldingen die onvoldoende aangeven wat er nu precies fout gaat. Ook klagen de apotheken over de wachttijd. Blijkbaar loopt het allemaal niet zo vlot.

Niet vermeld wordt dat in het beperkte aantal aangesloten ziekenhuizen het opvragen van medicatiedata niet “real time” gebeurt door beperkingen in ICT-apparatuur en de wachttijd bij het opvragen. Door het met een gekunstelde constructie opvragen van medicatiegegevens via het LSP door de ziekenhuisapotheek krijgt de specialist van polikliniekpatiënten deze door “prefetching”, het een dag van te voren opvragen. Daar is dan niets “real times” aan.

Ketenzorg

Om ketenzorg mogelijk te maken via het LSP moest een apart ketenzorgbericht gerealiseerd worden. Dat duurt nu al vijf jaar langer dan aangekondigd in het businessplan 2013 van VZVZ. In 2013 kwam er een programmaplan ketenzorg waarin een pilot in 2014 en realisatie in 2015 aangekondigd werd. Op dit moment, we leven nu in 2018, vindt op zeer beperkte schaal een pilot plaats in Friesland, nadat een Proof of Concept blijkbaar enig succes had. De uitkomst van de pilot zal zeker nog enige tijd op zich laten wachten.

Deze achtergronden worden niet vermeld in het kleine stukje over ketenzorg in hoofdstuk 8.8.

Geen compliancy

Met enige poeha stelt VZVZ in hoofdstuk 6.5.2 dat het LSP één van de eerste infrastructuren is die compliancy ingeregeld heeft. VZVZ stelt daarnaast dat het zorgaanbieders tegelijkertijd de zekerheid biedt dat ze het vragen van toestemming en het verwerken ervan goed doen.

Niets is minder waar. Er bestaat geen enkele verificatieplicht bij VZVZ over de opt-in-toestemmingen die aan VZVZ gemeld worden. Ook de zorgaanbieders blijken geen verificatieplicht

te hebben en kunnen straffeloos onterechte opt-in-toestemmingen noteren. Inmiddels is ook de autoriteit Persoonsgegevens ingeschakeld door burgers waarvan onterechte toestemmingen genoteerd waren.

Conclusie

Al met al kan ik gevoeglijk constateren dat VZVZ met veel omhaal van woorden en grafieken die deels onjuist, deels geflatteerde cijfers tonen probeert haar bestaansrecht op te poetsen. Het hele LSP-gebeuren blijft een zeer kostbare logge organisatie waaraan veel geld opgaat dat beter aan kleinschaliger oplossingen en gewoon aan de zorg besteed kan worden.

W.J. Jongejan, 24 april 2018

Groot, traag, duur en vol lucht en VZVZ pimpt het op: het LSP (deel 1)

Op 19 april 2018 zette de Vereniging van Zorgaanbieders Voor

Zorgcommunicatie(VZVZ), verantwoordelijk voor het Landelijk Schakelpunt(LSP) een rapport online op haar website. De titel is: "Rapport effecten en baten gebruik zorginfrastructuur". Met ronkende taal doet VZVZ voorkomen dat het LSP zeer goed draait en er boven verwachting gebruik van wordt gemaakt. Het lijkt erop dat VZVZ haar bestaansrecht aan haar financiers, de zorgverzekeraars, maar ook richting het zorgveld andermaal op wil poetsen. Diverse media berichtten er zonder kennis van zaken en zonder kritische blik over.

VZVZ maakt gebruik van manipulatie van cijfers, die in suggestieve grafieken worden getoond. Negatieve informatie staat weggemoffeld op onopvallende pagina's en nauwelijks vorderende projecten worden klein gebracht. Op de inhoud van het rapport is veel af te dingen. Met een nuchtere, kritische blik en kennis van eerdere door VZVZ zelf gepubliceerde getallen zijn grote gaten te schieten in rapport. Enkele vreemde vergissingen en aparte fouten zullen ook de revue passeren. In een tweetal artikelen zal ik met u het rapport doorlopen en de vinger op meerdere zere plekken leggen.

Cijfer- en grafiekenbrei

Met een overmaat aan getallen, percentages, deels vervat in grafieken kan VZVZ nauwelijks verhullen dat ruim 5 jaar na de private doorstart van het LSP eigenlijk relatief weinig is bereikt van wat men wilde. Het LSP is nu voornamelijk een medium om medicatieoverzichten op te vragen bij de voorschrijver of apotheek, omdat twee derde van de Nederlanders toestemming daarvoorgaf . Slechts één derde van de Nederlanders gaf toestemming om de huisartsgegevens(de Professionele Samenvatting) te delen. Het is duidelijk te zien in diverse grafieken, o.a de bovenste op pagina 14 waar eind 2017 6,4 miljoen huisarts-opt-ins vermeld staan. Op 17,2 miljoen Nederlanders is dat 37 procent.

Hypotheek

Ronduit vermakelijk is de bovenste grafiek op pagina 14. Daar staan het aantal unieke BurgerServiceNummers(BSN's), getekend voor apotheek, huisarts en totaal, over de jaren heen vermeld. Bij de legenda onder de grafiek blijkt het aantal unieke "hypotheek" in plaats van apotheek te staan. Nogal slordig zou ik zeggen, tenzij PR-man Alf Zwilling het als "easter egg" bedoeld heeft en een taart verschaft aan de vinder.

Gedraai met aangesloten huisartspraktijken

De afgelopen vijf jaar vergastte VZVZ de geïnteresseerde op de website met een overzicht genaamd "10 feiten over het LSP". Daarin gaf VZVZ steevast op dat 90 % van de huisartsenpraktijken aangesloten waren op het LSP. Op twee overzichten die ik in 2016 veilig stelde is dat te zien. Die overzichten zijn trouwens na de vernieuwing van de website van VZVZ in de herfst van 2017 niet meer terug te vinden. Nu komt VZVZ op pagina 13 in een tabel voor 2017 tot 77% aangesloten huisartsenpraktijken. Uit de voetnoot eronder blijkt dat VZVZ jarenlang bij huisartspraktijken keek naar het aantal unieke registratie abonneehouders(URA's). Dat is eigenlijk het aantal huisartsen die met een UZI-pas(toegangspas voor het LSP) geregistreerd staan als aangesloten genoteerd staan. Aangezien er meerdere huisartsen per (groeps)praktijk kunnen zijn, terwijl de praktijkhouder niet aangesloten is, zegt het aantal niets over de echte aantallen van aangesloten praktijken. **Jarenlang heeft VZVZ daarmee een voor haar te gunstig beeld geschetst over huisartsenpraktijken terwijl het percentage toch een stuk lager ligt.**

Geen gebruik bij wel aansluiting

Weggestopt op pagina 32 staat vermeld dat 58 % van de op het LSP aangesloten huisartsen het LSP helemaal niet gebruikt . Van hen die het wel doen blijkt 17% nooit de opgevraagde gegevens te gebruiken en 58% soms. Dat zijn toch echt zeer aanzienlijke aantallen die nu niet bepaald in het voordeel van het LSP pleiten. Men zou zich daarbij eens flink achter de

oren moeten krabben. VZVZ prijst zich gelukkig dat het percentage niet-opvragers afneemt maar het is nog steeds zeer substantieel.

Aantal toestemmingen en unieke BSN

De tweede grafiek op pagina 14 laat het aantal toestemmingen een unieke BSN's zien die geregistreerd staan. Met wel 20 miljoen in januari 2017. Dat aantal zegt helemaal niets. Een patiënt heeft altijd maar één huisarts, maar soms wel drie of vier apotheken. Bij allen dient een opt-in-toestemming gegeven te worden. Uitgaande van 17,2 miljoen Nederlanders(meldt VZVZ) kom je dan tot maximaal 17,2 miljoen huisarts-opt-ins en als we uitgaan van 3 apotheken per patiënt tot 3x 17,2=51,6 miljoen apotheek opt-ins. Opgeteld bij die van de huisartsen kom je dan tot wel 68,8 miljoen. Als er meer dan 3 apotheken per patiënt zijn en dat kan zeer wel(plaatselijke apotheken, ziekenhuisapotheken) ligt het getal nog hoger. Met andere woorden: het aantal zegt omdat het maximale volume aan niemand bekend is, niets. Hooguit zegt de stijging iets.

Leugenachtig

De bovenste grafiek op pagina 15 is ronduit leugenachtig. Deze geeft de toestemmingen(opt-ins) trend door de jaren heen weer. Daarin geeft de zwarte lijn die de toestemmingen bij de huisarts weergeeft door naar 11,8 miljoen, terwijl onder de grafiek het correcte aantal van 6,4 miljoen staat.(zie ook tweede alinea van dit artikel). Het lijkt erop dat de kleuren bij de legenda door elkaar gehusseld zijn, want de blauwe lijn met de toestemmingen polikliniekapotheken komt wel op 6,4 uit.

Wat de licht oranje lijn met "toestemmingen openbaar" betekent mag Joost weten, want dat staat nergens in de tekst uitgelegd. De PR- afdeling van VZVZ zal het wel weer op een drukfout gooien, maar ondertussen wordt een onterechte indruk gewekt bij de niet-kritische lezer.

Vervolg

Ik besprak nu slechts een deel van het gegoochel met getallen door VZVZ. Morgen zal ik in een vervolg-artikel verder ingaan op de overige cijfers, grafieken en onjuiste stellingen in dit rapport. Het is triest om te zien hoe koste wat kost gepoogd wordt een positief beeld over het LSP voor te schotelen.

W.J. Jongejan, 23 april 2018

De patiënt en het ziekenhuisinformatiesysteem EPIC: ervaringen

Ziekenhuisinformatiesystemen(ZIS-sen) hebben als doel om ziekenhuisbreed werkprocessen en verslaglegging te elektronisch te faciliteren. Het is daarbij de vraag of de patiënt als persoon, waarom het eigenlijk allemaal draait in de zorg, daar net zo de vruchten van plukt als de degenen die ermee werken. Nu is assortiment aan ZIS-sen niet bepaald groot te noemen. Eigenlijk zijn er maar twee hoofdspelers,

Chipsoft en EPIC, terwijl nog enkele kleinere spelers als SAP en Nexus een zieltogend bestaan leiden. Vandaag wil ik u eens als ervaringsdeskundige wat buitenissigheden laten zien van één van de hoofrolspelers: EPIC.

Met de ervaringen van een half jaar polibezoek bij meerdere soorten specialisten die EPIC gebruiken komt een vast patroon terug dat zich eigenlijk tijdens elk spreekuurbezoek voordoet. Die ervaring kon ik opdoen omdat het St. Antoniusziekenhuis half oktober 2017 in al zijn vestigingen(Nieuwegein, Leidsche Rijn en Woerden) overging op EPIC als ZIS. In Nieuwegein en Leidsche Rijn werkte men voordien met IntraZIS, een 20 jaar geleden in eigen beheer ontwikkeld systeem. In Woerden ging men vanuit Chipsoft over. Aangezien ik alle vestigingen van het ziekenhuis met een patiëntbezoek mocht vereren kon ik het gebruik van meerdere kanten observeren. Uiteraard zullen er opmerkingen komen als “startproblemen”, maar sommige zaken lijken me toch niet daartoe te behoren.

Horizon

Bij polikliniekbezoek viel op vier verschillende poli’s op dat er slechts sprake was van een horizon van twee maanden bij het maken van vervolgafspraken. Afspraken na die termijn kunnen niet gemaakt worden. Als je na drie maanden terug moet komen krijg je van het personeel te horen om twee maanden na het laatste polibezoek een keer te bellen om een afspraak een maand daarna te maken. Hopelijk is dan niet alles al volgepland, maar ja het kan niet anders.

Diezelfde horizon van twee maanden blijkt er ook te bestaan bij de planning voor een operatie. Nu in april krijg je te horen dat pas na eind juni de planning voor de volgende twee maanden van het operatieprogramma gemaakt kan worden. Enig zicht op wanneer een operatie gaat plaatsvinden als de wachtlijst langer is dan twee maanden, is er dus niet. Die planningshorizon van twee maanden is niet bepaald patiëntvriendelijk te noemen. Ik vermoed trouwens wel dat aan

de managementzijde van het EPIC de horizon langer is dan twee maanden. Anders is geen goede financiële administratie en planning van een ziekenhuis met EPIC mogelijk.

Even een order aanmaken

Tijdens meerdere polikliniekbezoeken verzochten specialisten mij om na het noteren van anamnese, lichamelijk onderzoek even niets tegen hen te zeggen. Ze vertelden met enige gêne dat ze dan “een order” moesten aanmaken. Ik begreep dat alle acties die een specialist wil uitvoeren, zoals het aanvragen van een röntgenfoto of MRI-scan als “een order” in het systeem moet komen. Ook na een half jaar gebruik is dat blijkbaar zo lastig dat iedere verstoring tijdens het aanmaken van de order desastreus is voor een correcte gang van zaken.

Bijzit

In een opleidingsziekenhuis is het tamelijk gewoon dat er tijdens een spreekuur naast de specialist een arts in opleiding bij het gesprek en onderzoek aanwezig is. Wieschetst mijn verbazing toen ik tijdens een recent polikliniekbezoek iemand in de spreekkamer trof die voorgesteld werd als ICT-medewerker. Het was me al opgevallen dat op andere plekken op de poli, o.a. bij diverse afspraakbureau ’s boventallige personeelsleden aanwezig waren. De aanwezigheid van de ICT-werker werd verklaard met de opmerking dat die diende om problemen tijdens het werken met het ZIS, EPIC dus, glad te strijken. Dus: handiger workflow voor te stellen dan de specialist bedacht had, uitleg van knoppen en opties etc. Blijkbaar is na een half jaar gebruik nog geen goede workflow bereikt. Ik hoop en verwacht dat deze mensen contractueel gehouden worden aan geheimhouding die gelijk is aan het medisch beroepsgeheim. Het was een aparte ervaring om op voornoemde gronden iemand erbij te hebben in de spreekkamer.

Geen combinatieafspraken

Bij het maken van een afspraak aan één van de balies ving ik

op dat helaas met EPIC niet mogelijk was combinatieafspraken te maken, iets wat met Chipsoft als ZIS voorheen wel kon. Dus op één ochtend tegelijk voor één patiënt afspraken maken bij meerdere specialisten zit er dus niet in. Heel erg klant(=patiënt)vriendelijk kwam dat niet op mij over.

Dichtgetimmerd

Eigenlijk hoor je maar heel weinig over problemen met de grote ZIS-ssen. Dat is het logische gevolg van het helemaal juridisch dichtgetimmerd zitten van uitingsmogelijkheden van ziekenhuismedewerkers over zo'n systeem. Klachten mogen vanwege non-disclosure-bepalingen in de contracten tussen ziekenhuizen en de ZIS-leveranciers niet individueel of collectief naar buiten worden gebracht. Alle communicatie erover moet via de directie lopen die ook weer gehouden is te handelen volgens contractuele bepalingen. Heel af en toe komt het toch, maar dan anoniem, naar buiten en zie je het soms in de berichtgeving van bijvoorbeeld Nictiz over de appreciatie van ZIS-sen in de jaarlijkse eHealth-monitor.

Gratis advies

Mochten mijn opmerkingen en bevindingen als zuur en te kritisch overkomen, dan is mijn advies om bij alles wat men aan elektronische systemen in een ziekenhuis heeft ook het patiënten perspectief te betrekken. Bovendien zou ik zeggen, beschouw mijn opmerkingen als gratis advies om dingen anders en beter in te richten.

W.J. Jongejan

Wat als de CT- of MRI-scanner gekaapt is door malware?

In mei 2017 hebben we kunnen zien hoe het Wannacry-virus huishield bij de National Health Service(NHS) in het Verenigd Koninkrijk. Deze malware slaagde erin grote aantallen ICT-systemen van zorgaanbieders plat te leggen dan wel ernstig te verstoren. De National Audit Office bracht er verslag over uit op 24 oktober 2017. Onder de aangedane systemen waren ook MRI-scanners, die evenals CT-scanners, een uiterst belangrijke rol spelen bij onderzoek met beeldvormend technieken in ziekenhuizen. Deze apparaten hebben vaak een op Windows gebaseerd eigen besturingssysteem en zijn gekoppeld aan het ziekenhuisnetwerk.

Een onderzoeksgroep aan de Ben-Gurion University of the Negev, in Beer-Sheva(Israël) publiceerde in maart 2018 een artikel over dit onderwerp, genaamd: "Know your enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices." In het artikel beschrijven de onderzoekers een uitgebreide risico analyse over de kwetsbaarheid van MRI- en CT-scanners, als Medical Imaging Devices(MID). Ze beschrijven een aantal kwetsbaarheden en potentiele doelen, waardoor met deze appraten niet meer gewerkt kan worden. Dat zou een ramp zijn, omdat MID's zeer intensief in de zorg gebruikt worden voor diagnose, behandeling en preventie van ziekten. In mijn bijdrage zal ik de inhoud van het artikel in het kort bespreken.

Grootste risico

Van de MID’s lopen de CT-scanners het grootste risico van slag te worden gebracht door malware. Dat heeft te maken met de centrale rol die deze apparaten spelen bij beeldvormend onderzoek in de acute zorg. Daarom focusten de onderzoekers zich na een beschrijving van de rol van de MID’s in de hedendaagse zorg en een beschrijving van de Wannacry-cyberaanval op de problemen die met CT-scanners kunnen ontstaan bij dat soort aanvallen.

Vier categorieën aanvallen

De onderzoekers beschrijven een viertal ernstige verstoringen van CT-systemen die zij zelf hebben kunnen uitproberen. Het gaat bij de aanvalsgevolgen om gevaar voor de patiënt die in het apparaat ligt, maar ook voor andere patiënten. Daarnaast kan ook de technische staat van een CT-scanner ernstig aangetast worden.

1. Een CT-scanner opereert op basis van een configuratie-bestand dat in de besturingscomputer opgeslagen is . Het zorgt voor een correcte werking van de scanner. Door het aanpassen van dat bestand kan de hele werking van de scanner gemodificeerd worden, bijv. de hoeveelheid straling die de röntgenapparatuur in de scanner afgeeft.
2. De MID’s hebben een flink aantal elektromotoren aan boord die instructies krijgen vanuit de computer met het specifieke besturingssysteem. Het ongeautoriseerd overnemen van de controle over deze motoren kan ongewenste bewegingen van het apparaat ten gevolge hebben. De patiënt in de scanner kan daar grote schade van ondervinden, maar ook de scanner zelf.
3. Uit de ruwe data die een CT-scanner tijdens een onderzoek produceert worden door een bij de scanner horend ICT-systeem de beelden gevormd en aan de betreffende patiënt gekoppeld. Na het maken van de beelden worden die volgens een specifiek protocol(DICOM=

Digital Imaging and Communications in Medicine) verder getransporteerd en opgeslagen. Een aanval op de in dit punt genoemde systemen kan er toe leiden dat het onderzoek bij een patiënt verstoord wordt en een tweede onderzoek met daardoor extra stralingsbelasting nodig is. Bij een meer diepgaan verstoring kan het scanresultaat veranderd zijn, waardoor het ook zeer moeilijk te zeggen is wat er fout is. Tenslotte kan met een nog gehaaidere aanval het scanresultaat aan een andere persoon gekoppeld worden.
4. Ook kan zogenaamde ransomware bestanden versleutelen, waarna een geldsom(evt in cryptocurrency) geëist kan worden om die weer ontsleuteld te krijgen.

Preventie

De onderzoekers stellen dat met cyberaanvallen op MID's steeds meer rekening moet worden gehouden en dat leveranciers van deze apparatuur en andere zorg-hard-/software voor een enorme uitdaging staan. Gebruikers dienen zich bewust te zijn van de risico's en het mechanisme achter de potentiële aanvallen moet begrijpen om ze te voorkomen. De Wannacry-cyberaanval kon zo uitgebreid toeslaan omdat veel software binnen de ziekenhuizen, ook de besturingssystemen van CT- en MRI-scanners onvoldoende geüpdatet waren. Sommige systemen draaiden nog onder Windows XP! Het probleem met de scanners is dat de ontwikkelingstijd van nieuwe scanners vaak lang duurt en dat een eenmaal in het begin gekozen besturingssysteem vaak niet zomaar overgezet kan worden naar een nieuw als het eerste door bijvoorbeeld Microsoft uitgefaseerd wordt. Het installeren van krachtige antivirus-software kan wel iets betekenen, maar is beslist niet afdoend in het geval van verouderde besturingssystemen. Toch blijft het van eminent belang om bestaande systemen continu van nieuwe patches te voorzien.

Oplossingsrichting

De auteurs stellen als extra oplossingsrichting een meer functionele voor. Zij stellen naast de eerder genoemde maatregelen voor om het dataverkeer van de besturende en data-verwerkende systemen met de scanner zelf continu te monitoren en met artificiële intelligentie(lerende systemen) te beoordelen. Daardoor kunnen afwijkingen van bestaande processen gedetecteerd worden en ingegrepen worden voor er iets misgaat.

Uitval van één MID-systeem door malware of andere vorm van hacken kan een heel ziekenhuissysteem platleggen. Maar omgekeerd geldt ook dat een gecompromitteerd ziekenhuis-informatiesysteem beeldvormende apparatuur volkomen plat kan leggen.

W.J. Jongejan

Parnassia groep zet wereld op zijn kop bij beantwoording Kamervragen over ROM

Bij de beantwoording van Tweede Kamer vragen van het SP-kamerlid Kooiman aan de minister van VWS blijkt de GGZ-instelling Parnassia Groep de wereld op zijn kop te zetten. Dit doet deze instelling in antwoorden op vragen van het ministerie over de hervatting van ROM-gegevens aanlevering aan de Stichting Benchmark Geestelijke Gezondheidszorg(SBG). Ze stelt dat het vragen van expliciete toestemming hiervoor aan de cliënten leidt tot een toename van de administratieve lasten. Parnassia probeert hier gebruik te maken van de pogingen tot bestrijding van onnodige regelgeving die op het ogenblik gaande is onder het auspiciën van (Ont)regel de zorg. Daarbij maakt Parnassia een zeer grote, maar essentiële fout door met een beroep op deze beweging een essentieel recht van de cliënt in de GGZ om zeep te helpen. In de Kamervragen verzoekt het Kamerlid Kooijman aan de minister van VWS te antwoorden op het bericht dat de GGZ-instelling Parnassia Groep Routine Outcome Monitoring(ROM)-data deelt met SBG. Meer specifiek gaat het om de hervatting van de aanlevering van die gegevens aan SBG op basis van het zeer discutabel begrip “veronderstelde toestemming”.

Expliciete toestemming

De vragen worden in het Kamerstuk beantwoordt door de staatssecretaris voor VWS Paul Blokhuis. Deze stelt zich net als de vorige minister van VWS, Edith Schippers, op het standpunt dat voor het doorsturen van de ROM-data naar SBG en na 1 januari 2019 naar de rechtsopvolger daarvan, AKWA, expliciete toestemming van de cliënt noodzakelijk is. AKWA staat voor Alliantie KWAliteit in de zorg en is het nieuwe kwaliteitsinstituut voor de GGZ. Tot deze uitspraak kwam de staatssecretaris al eerder en hij bevestigt dit in het antwoord op vraag 2 in de beantwoording van de Kamervragen.

Expliciete toestemming is absoluut nodig bij het be-/verwerken en gebruiken van medische persoonsgegevens door partijen die niet direct betrokken zijn bij een behandeling. De ROM-data zijn ondanks pseudonimisering gewoon nog bijzondere

persoonsgegevens en SBG en de rechtsopvolger in de nabije toekomst zijn geen direct betrokkenen bij de behandeling.

Zeer vreemde standpunten

In zijn antwoord op de vragen 3 en 4 stelt Blokhuis dat hij geadviseerd heeft om voor de zekerheid met expliciete toestemming te werken. Om dan vervolgens, vreemd genoeg, genoegen te nemen met het verhaal van Parnassia Groep dat de cliënten geïnformeerd worden en ervoor kunnen kiezen om niet deel te nemen. De staatsecretaris legt dat in de beantwoording van vraag 9 nog eens uitgebreid uit. Dat is echter helemaal geen expliciete toestemming maar een opt-out-constructie die het recht va de cliënten ontkracht.

Ondanks de ferme uitspraak over de expliciet toestemming onderneemt het ministerie zelf geen acties maar verwijst zij voor handhaving in het antwoord op vraag 5 en 7 door naar de Autoriteit Persoonsgegevens(AP) als zijnde de toezichthouder op dit terrein. Deze heeft al eerder bij vragen over de ROM-doorlevering zonder expliciete al getoond er een beleid van vertraging en rekken erop na te houden zonder echt tot maatregelen te komen.

Grote fout

Blokhuis maakt een zeer grote fout door in het antwoord op vraag 8 te stellen dat de ROM-gegevens niet gedeeld worden met derden, ook niet met zorgverzekeraars. SBG is als ontvanger van de ROM-data **WEL DEGELIJK** een derde, omdat het een partij is die niet rechtstreeks betrokken is bij de behandeling. Een derde die bovendien voor honderd procent door de zorgverzekeraars betaald wordt. Dat zorginstellingen, in het antwoord van Blokhuis, niet gekort worden door de zorgverzekeraar is een situatie die vooralsnog bestaat vanwege de onrust over de aanlevering van ROM-data aan SBG. Contractueel is echter vastgelegd dat zorgaanbieders gekort worden bij onvoldoende aanlevering van data. De

zorgverzekeraars beseffen maar al te goed dat nu strafkortingen hanteren alleen maar het vuur verder kan doen aanwakkeren

Gotspe

Dat Parnassia Groep op vragen van het ministerie over deze materie stelt dat het vragen van expliciete toestemming bijdraagt aan een toename van de administratieve lasten is met recht een gotspe te noemen. Het geven van een expliciete toestemming om zelf te bepalen of medische gegevens doorgestuurd worden aan partijen die niet betrokken zijn bij de behandeling, valt niet onder enige verzwaring van administratieve lasten. Het is een onvervreemdbaar grondrecht waar niet aan getornd dient te worden. Het is uitermate kwalijk te noemen dat bestuur en directie van Parnassia Groep verwijzen naar “toename van administratieve lasten” in een tijd waarin die ter discussie staan. Het komt over als het op volkomen onterechte wijze mee willen surfen op een beweging van werkers in de zorg die zich terecht zorgen maken over de enorme regelgeving.

W.J. Jongejan

Ook na aanpassing Wiv blijft inbreuk in medische datasystemen mogelijk

Afgelopen dinsdag 10 april 2018 discussieerde de Tweede kamer over de reactie van het kabinet op de uitslag van het raadgevend referendum over de Wet op de inlichtingen- en veiligheidsdiensten(Wiv2017). Het debat leverde nu niet bepaald een enorm vuurwerk op. Dat zou je wel verwachten bij de zeer magere, en waarschijnlijke vooraf al ingecalculeerde aanpassingen die kabinet in de brief met de reactie ventileerde. De beloofde aanpassingen, nieuwe beleidsregels genoemd, betreffen enkele cosmetisch ingrepen, die de wet eigenlijk niet echt veranderen. In de "waarborgen in de uitvoeringspraktijk" komt in punt 5 de omgang met medische gegevens ter sprake. Op dat punt is helemaal niets gewijzigd en komt het kabinet met een uitleg die gerichte inzage in medische datasystemen niet uitsluit. Men komt met een uitleg over het verwerken van medische gegevens die in de aanloop naar het referendum al vaker te horen was. Dat kwam dan uit de mond van bewindslieden en (oud)hoofden van AIVD en MIVD. Ondanks de geruststellend bedoelde formulering in punt 5 is er nog steeds met de Wiv2017 een duidelijk koerswijziging ingezet, namelijk het in principe legaal kunnen binnendringen in medische data(transport)systemen. Ik schreef over dit onderwerp een vijftal stukken. **Zie voor de link ernaar aan het einde van dit artikel.**

Wat zegt het kabinet?

In de brief aan de Tweede Kamer zegt het kabinet:

5. ***Omgang medische gegevens***

De Wiv2017 (artikel 19) kent een bijzondere status toe aan de

verwerking van medische gegevens. De verwerking van persoonsgegevens wegens iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven vindt niet plaats. Dit kan alleen in aanvulling op de verwerking van andere gegevens, dus als iemand onderwerp is van lopend onderzoek en de medische gegevens het sluitstuk vormen op de informatie die de diensten nodig hebben om een dreiging goed in beeld te brengen. Dit geldt dus ook voor de eventuele verwerking van medische gegevens uit de dataset verkregen door onderzoeksopdracht gerichte (OOG)-interceptie op de kabel. Indien de diensten op medische gegevens stuiten die zij niet mogen inzien, zullen zij deze direct verwijderen. De CTIVD houdt toezicht of de diensten niet ten onrechte medische gegevens verwerken en rapporteert hierover aan de Tweede Kamer.

Wat staat hier?

Ogenschijnlijk lijkt het heel mooi dat gesteld wordt dat gegevens over iemands gezondheid niet verwerkt worden. Om daar dan in de volgende zin meteen aan toe te voegen dat het wel mag in aanvulling op de verwerking van andere gegevens en de medische data als sluitstuk dienen op informatie die de diensten nodig hebben om een dreiging goed in beeld te brengen. Men doelt dan niet uitsluitend op medische data die in het kader van een OOG-interceptie verkregen zijn. De bevoegdheid om gericht aan die aanvullende data te komen ontlenen de diensten, met de Wiv 2017 in de hand, aan artikel 45 daarvan. Daarin staat dat het mogelijk is dat de diensten gericht data(transport)systemen mogen binnendringen zonder dat daarbij een uitzondering vermeld is voor medische data(transport)systemen. Gericht hacken en zoeken in medische data- en datatransportsystemen is wel degelijk gepermitteerd met de wet.

Medisch beroepsgeheim

Er zijn mensen die zeggen, dat je je niet druk moet maken over

de theoretische mogelijkheid dat een dienst medische data gericht gaat zoeken en daarvoor medische systemen doorzoekt. Het gaat daarbij om het van staatswege bewust doorbreken van het medisch beroepsgeheim. Aan zeer veel kanten staat het medisch beroepsgeheim onder druk door toedoen van de landelijke, maar ook de lokale overheid. Ik hoef daar alleen maar de perikelen rond de jeugdzorg onder de aandacht te brengen, waar wijkteams en andere overleggroepen over medische data wensen te beschikken zonder dat meerdere deelnemers gebonden zijn aan een beroepsgeheim. Daarbij komen medische data ook wel onder ogen van onbevoegden bij die overheden. Ook bij zorgverzekeraars spelen (dreigende) inbreuken op het medisch beroepsgeheim,.

Elke aantasting is er één

Juist omdat het medisch beroepsgeheim aan veel kanten onder druk staat, is het van belang om elke keer als dat dreigt te gaan gebeuren aan de bel te trekken. Zeker nu het met wetgeving rond de diensten een principiële discussie betreft. Door de Wiv2017 gaat het daarbij om het legaliseren van mogelijke inbreuken door het niet noteren van beperkingen in de wet ten aanzien van medische data. Groen Links deed nog een halfhartige poging om het medisch beroepsgeheim in de aanpassing van de Wiv gegarandeerd te krijgen, maar liet het hoofd snel hangen.

Het is ook weer jammer om te constateren dat ook nu weer de Koninklijke Nederlandse Maatschappij ter bevordering van de Geneeskunst(KNMG) publiekelijk niets van zich liet horen tussen het bekend worden van de referendumuitslag en het Kamerdebat. Weer een gemiste kans dus. De KNMG dient zich ten allen tijde publiekelijk als bewaker van het medisch beroepsgeheim op te stellen en niet halfhartig te opereren.

W.J. Jongejan

5 oktober 2017: Referendum sleepwet noodzakelijk i.v.m.

aantasting medisch beroepsgeheim

8 oktober 2017: KNMG en LHV beseffen nu pas impact sleepwet op medisch beroepsgeheim

22 januari 2018: KNMG probeert alsnog patiëntdata beschermd te krijgen in kader van sleepwet

7 februari 2018: Flink geschut in stelling pro sleepwet. Serieuze opmaat naar referendum

23 maart 2018: Nasleep sleepwetreferendum meeslepend met onverwachte wendingen

---

Kwaliteitsstatuut GGZ faciliteert benchmarking met ROM en schending beroepsgeheim

Na de ophef over het verzamelen en verwerken van ROM-data door de Stichting Benchmark GGZ(SBG) in 2017 liet GGZ Nederland met veldpartijen uit de geestelijke gezondheids-zorg(GGZ)[i] op 18 oktober 2017 weten dat de verwerking van die data weer hervat kon worden. Het kon volgens hen gebeuren op basis van "veronderstelde toestemming". Dat was een cosmetische operatie. Men veranderde gewoon op papier het doel van het

verzamelen en be-/verwerken van Routine Outcome Monotoring(ROM)-data. Van benchmarking en zorginkoop als doel werd het nu kwaliteitsverbetering. Dat wil men bereiken door de resultaten van de ROM-verwerking terug te sluizen richting behandelaars.

In de marge meldde men dat het Kwaliteitsstatuut, vanaf 1 januari 2017 verplicht voor de gehele geneeskundige GGZ, opnieuw doorgelopen zou worden om te zien of men met de veranderde doelstelling het statuut niet moest aanpassen. Naar nu blijkt, bij het lezen van versie 1.1 **(d.d. 26 maart 2018)** van het model Kwaliteitsstatuut GGZ, staat nog steeds de verplichting tot aanleveren van ROM-data aan SBG overeind. Ook de doelstelling is onveranderd: het aanleveren van ROM-gegevens aan SBG die op geaggregeerd niveau beschikbaar zijn ten behoeve van benchmarking.

Kwaliteitsstatuut

GGZ organisaties van patiënten, zorgaanbieders en zorgverzekeraars[ii] hebben gezamenlijk het model Kwaliteitsstatuut GGZ ontwikkeld en aangeboden aan het Zorginstituut Nederland voor opname in het Kwaliteitsregister. Op 29 maart 2016 heeft de raad van bestuur van Zorginstituut Nederland besloten het model Kwaliteitsstatuut voor de ggz als een professionele standaard op te nemen in het register. Zoals gezegd werd het Kwaliteitsstatuut per 1-1-2017 van kracht voor alle aanbieders van ‘geneeskundige ggz’, dat wil zeggen: generalistische basis-ggz en gespecialiseerde ggz binnen de Zorgverzekeringswet.

ROM-men in recente versie

In de meest recente versie van het model Kwaliteitsstatuut staat voor de vrijgevestigden in sectie II(blz 17)

- Dat de vrijgevestigde een kopie van de overeenkomst met de Stichting Vrijgevestigden ROM-men(SVR) voor de aanlevering van ROM-gegevens overlegt.

En voor de GGZ-instellingen in sectie III (blz.24):

- Dat de zorgaanbieder ROM-gegevens aanlevert aan SBG die op geaggregeerd niveau beschikbaar zijn ten behoeve van **benchmarking**
- Dat de zorgaanbieder een kopie overlegt van de overeenkomst met SBG voor het aanleveren van ROM-gegevens.

Er is dus ondanks de cosmetische operatie die in de herfst van 2017 doorgevoerd werd niets, maar dan ook niets veranderd. Noch aan de vastgelegde verplichting tot aanlevering noch aan de doelstelling van de ROM-verzameling bij SBG veranderde ook maar iets. Het modelstatuut toont eens te meer aan dat het in een verklaring vastleggen van de doelwijziging slechts een cosmetische operatie was.

Schending beroepsgeheim

Op 29 maart 2018 schreef ik al in een artikel dat het model Privacyreglement GGZ zowel het medisch beroepsgeheim als het toestemming geven door de patiënt voor het buiten de GGZ-instelling verwerken van zijn/haar ROM-data volledig buiten spel zet. Datzelfde kan gezegd worden van het model Kwaliteitsstatuut GGZ. Daarin onderscheidt men ook weer de drie lagen die ook in het model Privacyreglement vermeld staan: de cliënt, de zorgverlener(therapeut in dienst van een instelling) en de zorgaanbieder. De begrippenlijst in beide documenten is in dit kader veelzeggend.

Met de zorgaanbieder wordt de GGZ-instelling als rechtspersoon bedoeld, die vertegenwoordigd wordt door de directie en het bestuur van de zorginstelling. Net als in het model Privacyreglement is het in het Kwaliteitsstatuut de zorgaanbieder en niet de zorgverlener die het contract met SBG sluit. En is het ook de zorgaanbieder(lees directie en bestuur) en niet de zorgverlener(therapeut)die besluit dat ROM-data aan SBG geleverd worden voor benchmarking.

Geen toestemming

Het begrip toestemming en ook het begrip “gerichte toestemming” staan wel apart vermeld in het Kwaliteitsstatuut. Men laat dat bijvoorbeeld slaan op het door de cliënt toestemming geven aan de zorgverlener om zorg te gaan verlenen. Maar nergens staat in het statuut een vermelding van een expliciete toestemming die nodig is voor het verstrekken, doen be-/verwerken en gebruiken van medische persoonsgegevens door partijen die niet direct betrokken zijn bij een behandeling. En dat zijn de ROM-data nu eenmaal ook al zijn ze dubbel gepseudonimiseerd. De beslissing om de ROM-data te leveren aan SBG neemt de zorgaanbieder(lees: directie en bestuur) dus en niet de zorgverlener(de therapeut) en zelfs niet de cliënt. Gezien het voorgaande is het dus overduidelijk, dat het model Kwaliteitsstatuut en het Privacyreglement als twee loten aan dezelfde stam gezien moeten worden.

Niet gezien?

Het is de vraag waarom de in de alliantie met GGZ Nederland en Zorgverzekeraars Nederland samenwerkende organisaties die vermeld staan in de tweede voetnoot niet zelf de manco’s in beide stukken gezien hebben en corrigerend gehandeld hebben. Ook in de meest recente versie(eind maart 2018) van het model Kwaliteitsstatuut staat exact hetzelfde over SBG als in de versie uit 2016. De vraag dringt zich dan ook op hoe sterk die organisaties van beroepsbeoefenaren en cliënten ingekapseld zitten in bestuurlijke constructies waarin kritische geluiden niet meer geuit kunnen worden.

W.J. Jongejan

[i] MIND, NVvP, NIP, P3NL, V&VN en MEER GGZ

[ii] GGZ Nederland, de Nederlandse Vereniging voor psychiatrie, de Landelijke vereniging van Vrijgevestigde Psychologen & Psychotherapeuten, het Nederlands Instituut voor

Psychologen, het Landelijk Platform GGZ, Platform MEER GGZ, InEen, Verpleegkundigen en Verzorgenden Nederland , P3NL de federatie van psychologen, psychotherapeuten en pedagogen en Zorgverzekeraars Nederland.

IGJ schuift melding over ontbreken verificatieplicht VZVZ door naar AP

Op 5 februari 2018 schreef ik op deze website een bijdrage met als titel "IGJ dient verificatieplicht tav toestemming delen medische data breder af te dwingen". Het ging over de vraag van mij aan de Inspectie voor de Gezondheidszorg en Jeugd(IGJ) om de verificatieplicht die zij aan het Isala-ziekenhuis in Zwolle oplegde breder te trekken. Daarbij vroeg ik de IGJ om stappen te zetten richting de Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ) vanwege het op enige schaal plaats vinden van onterechte opt-in-toestemmingen voor het delen van medische informatie via het Landelijk SchakelPunt(LSP). Door een verificatieplicht kan het onterecht noteren van opt-in-toestemmingen voor het delen van medische gegevens over het LSP de kop ingedrukt worden. Over het onterecht doen noteren van opt-in-toestemmingen bij apotheken voor medicatiegegevens deed de burgerrechtenvereniging Vrijbit al in de herfst van

2017 twee handhavingsverzoeken aan de Autoriteit Persoonsgegevens(AP). In een reactie op mijn verzoek aan de IGJ heeft de coördinerend specialistisch inspecteur eHealth, drs. J.W. Krijgsman, mij op 15 maart 2018 laten weten dat de IGJ mijn verzoek niet in behandeling kon nemen en doorgeschoven heeft richting de AP.

Formeel

De IGJ kon bij het Isala-ziekenhuis hen aanspreken op basis van de Wet aanvullende bepalingen verwerken persoonsgegevens, en wel artikel 15a daarvan. De Wabvp bepaalt dat een zorgaanbieder gegevens van de cliënt slechts beschikbaar stelt via een elektronisch uitwisselingssysteem, voor zover de zorgaanbieder heeft vastgesteld dat de cliënt hier uitdrukkelijk toestemming voorheeft gegeven. De Wabvp richt zich expliciet op zorgaanbieders als bedoeld in de Wet kwaliteit, klachten en geschillen zorg(Wkkgz). Formeel gezien is VZVZ geen zorgaanbieder in de zin der wet, maar een be-/ verwerker van medische gegevens. Om die reden kan de IGJ niet toezien op het handelen of nalaten van de VZVZ zoals verwoord in mijn verzoek aan de IGJ.

AP

De inspecteur van de IGJ gaf terecht aan dat hij de AP de bevoegde toezichthouder acht over VZVZ. Na telefonisch overleg met mij heeft hij dan ook contact opgenomen met de AP met het verzoek aldaar de behandeling van het verzoek over te nemen. De AP heeft daartoe inmiddels met mij contact opgenomen, onder andere met het verzoek of ik mij wil voegen bij de twee handhavingsverzoeken van de burgerrechtenvereniging Vrijbit of dat ik een separaat handhavingsverzoek wil doen. Daarover zal ik ze binnenkort berichten.

Grote kans

Vrijbit is trouwens nog steeds in afwachting van een formele uitspraak van de AP over de twee hierboven genoemde

handhavingsverzoeken. Daarbij is de wettelijke reactietermijn voor de AP weer eens een keer ruim overschreden. De afwijzing die de IGJ op mijn melding deed op formele gronden opent echter wel een grote kans voor Vrijbit om zich tot de IGJ te wenden met een handhavingsverzoek ten aanzien van apotheken die ten onrechte op enige schaal onterechte opt-in-toestemmingen noteren in hun systemen. De apotheken vallen immers wel onder de Wkkgz en zijn ook door hun beroepsorganisatie, de Koninklijke Nederlandse Maatschappij ter bevordering van de Pharmacie(KNMP) uitgebreid geïnstrueerd hoe ze met die wet dienen om te gaan. Omdat de apotheken onder de Wkkgz vallen zijn ze derhalve aan te spreken op een verificatieplicht op basis van de Wabvp. De IGJ kan de overtredende apotheken dwingen tot een verificatieplicht bij het vastleggen van opt-in-toestemmingen. Daardoor kan afgedwongen worden dat de burger actief per gewone post of email ingelicht wordt door de apotheek als er iets in de opt-in-status verwijderd wordt.

We gaan het zien.

W.J. Jongejan