

VZVZ verandert heimelijk essentiële punten in gebruiksovereenkomst LSP



[Op de website van VZVZ word per 23 februari gemeld](#) dat het addendum ten aanzien van de aansprakelijkheid ingevoegd is in de Algemene Voorwaarden. Het addendum is medio 2015 uit onderhandeld tussen de Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ) en de Landelijke Huisartsen Vereniging(LHV). Ik berichtte hier over op deze website [op 11 juni](#), [18 juni](#), [14 juli](#) en [24 september](#) 2015 over. Inderdaad is in de Algemene Voorwaarden te zien dat het in september 2015 gepubliceerde Addendum in de Algemene Voorwaarden is ingebouwd. Er staat ook een link op de website naar de nieuwe gebruiksovereenkomst die ingaat per 1 januari 2016.

Wat VZVZ NIET op haar website vermeld is dat de gebruiksovereenkomst voor (apothekhoudende) huisartsen, Huisartsenposten en Apotheken, die de op het Landelijke SchakelPunt(LSP) aangesloten met het VZVZ-Servicecentrum sluiten, op een aantal punten wezenlijk veranderd is.

Geringe betekenis

De door VZVZ genoemde verzekering voor bij haar geclaimde schade aan een patiënt door malfunctie van het LSP stelt weinig voor. Het is een zogenaamde regres-verzekering. Men mag VZVZ pas financieel aansprakelijk stellen als een schadeclaim bij de eigen verzekering is ingediend en daar geen schade is

uitgekeerd. Ik schreef daar op 24 september 2015 al over.

Markering wijzigingen

Om een goede beoordeling van de verschillen tussen [de oude Gebruiksovereenkomst d.d. 10 mei 2013](#) goed te kunnen zien, zijn door mij in [de nieuwe Gebruiksovereenkomst d.d. 01-01-2016](#) de verschillen gemarkeerd. Voor een deel zijn het kleine tekstuele aanpassingen, maar een aantal is toch zeer essentieel te noemen.

Begrippenlijst

In de begrippenlijst zijn de items Datalek, Patiënt, Vergoedingsreglement, VZVZ Derdengelden toegevoegd en werd het begrip ZorgServiceProvider(ZSP) vervangen door Goed Beheerd Zorgnetwerk(GZN). Het zijn deels aanpassingen op basis van veranderde wetgeving, zoals het melden van datalekken, deels praktische aanpassingen. Opvallend is dat in alle eerdere versies de patiënt niet in de begrippenlijst voorkwam, terwijl de datacommunicatie toch echt voor die bedoeld lijkt. Het punt datalek is verder uitgewerkt in punt 4.7 van de gebruiksovereenkomst. Daar staat dat de gebruiker per ommekeer melding maken moet aan VZVZ of het Servicecentrum bij vermoeden van of vastgesteld zijn van een datalek in verband met zijn/haar aansluiting op en gebruik van het LSP. De Autoriteit Persoonsgegevens dient dus niet alleen ingelicht te worden, maar ook voornoemde instellingen moeten er weet van hebben.

Voorlichting

In de artikelen 3 tot en met 7 zijn veel essentiële wijzigingen doorgevoerd. Artikel 3.3 is toegevoegd over de wijze van voorlichting aan de patiënt bij het verkrijgen van de opt-in-toestemming .

“3.3 Gebruiker zal de patiënt zoals bedoeld in artikel 3.2 voorafgaand aan het vragen van de toestemming informeren over

de reikwijdte van de toestemming op de door VZVZ/ Servicecentrum aan hem voorgeschreven wijze. Daarbij maakt Gebruiker gebruik van het informatiemateriaal van VZVZ of informatie van gelijke inhoud.”

Ongetwijfeld is dit punt toegevoegd naar aanleiding van de rechtszaak van de Vereniging Praktijkhoudende Huisartsen tegen VZVZ over het LSP. Daarin is adequate voorlichting van de patiënt een belangrijk item. In het hoger beroep verweerde VZVZ zich uitgebreid met verwijzingen naar eigen voorlichtingsmateriaal, dat overigens in de loop der tijd op meerdere punten aangepast werd.

Geen melding van inzage aan gebruiker

Een veel ingrijpender item is het weglaten van het woord “gebruiker” in de tweede zin van artikel 4.6.

Daar staat nu:

“Ten behoeve van de informatiebeveiliging en de uitoefening van patiëntenrechten zal een gebruiksregistratie in stand worden gehouden. Servicecentrum zal gegevens uit de gebruiksregistratie namens de VZVZ verstrekken aan patiënten op wie de gegevens betrekking hebben, conform wettelijke voorschriften. Aan anderen worden de gegevens niet verstrekt, behoudens een wettelijke verplichting daartoe.”

In de versie uit 2013 staat dat er een gebruiksregistratie plaatsvindt van de raadplegingen van medische data van een patiënt via het LSP en melding plaatsvindt aan de patiënt EN de gebruiker.

Raadpleging van een dossier wordt niet automatisch aan een patiënt gemeld, maar [deze moet actief een overzicht aanvragen of actief zich abonneren op de email-service](#) van VZVZ over die inzagen.

Indien de patiënt zulks niet zou doen en de raadpleging ook

aan de gebruiker(zijnde brongegevens houdende zorgverlener) gemeld wordt is deze laatste ook in staat te controleren of de bevraging terecht was. Door de gebruiker te schrappen in de tekst is er sprake van uitsluiting van de brondossier houdende zorgverlener bij het controleproces.

Vergoedingen

In artikel 5 is artikel 5.2 toegevoegd. Dat gaat over de aanspraak op vergoeding via het Vergoedingenreglement. De rechten op de eenmalige en jaarlijkse vergoedingen worden hierin vastgelegd.

Eenzijdige macht

In artikel 6 over de duur van de overeenkomst en de beëindiging is onder 6.4 een nieuw artikel ingebracht.

“6.4 Servicecentrum is gerechtigd de Overeenkomst met onmiddellijke ingang te beëindigen wanneer zij op grond van eigen waarneming, waarneming door VZVZ of op basis van de melding van Gebruiker zoals bedoeld in 3.7, aantoonbaar heeft vastgesteld dat Gebruiker wezenlijk niet langer aan de Overeenkomst, de Standaarden dan wel de Nederlandse wetgeving voldoet en/of kan voldoen. Deze opzegging leidt niet tot enige schadeplichtigheid jegens Gebruiker van VZVZ en/of Servicecentrum. Servicecentrum houdt bij toepassing van dit artikellid steeds rekening met de belangen van de zorgverlening en de belangen van de bescherming van de persoonlijke levenssfeer van de patiënt.”

Hier staat met zoveel woorden dat het Servicecentrum op basis van eigen “waarneming” of die van VZVZ dan wel door “een melding” van een gebruiker(een andere zorgverlener?) met onmiddellijke ingang het dataverkeer met de gebruiker kan doen stoppen. Gaat VZVZ op basis van via andere gebruikers verkregen informatie iemand schrappen? Daaraan wordt een tekst toegevoegd dat die opzegging niet leidt tot enige schadeplichtigheid jegens gebruiker van VZVZ of het

Servicecentrum. De gebruiker wordt door ondertekening van de gebruiksovereenkomst geacht het hiermee eens te zijn. De gebruiker wordt dus geacht te tekenen voor een eenzijdig machtsmiddel en tegelijk voor het laten varen van een financiële verhaalsmogelijkheid. Hierdoor worden de rechten van de gebruiker(de aangesloten zorgaanbieder) wezenlijk beknot.

In artikel 7.7, dat toegevoegd is , wordt als pleister op de wonde bij opzegging door VZVZ of door ontzetting uit het lidmaatschap een beroepsmogelijkheid van een maand gegeven bij de ledenraad van VZVZ. Opvallend dat het beroep niet mogelijk is bij de leiding van VZVZ, maar bij de ledenraad. Het is maar helemaal de vraag of de ledenraad dwingend iets kan besluiten tegen de leiding van VZVZ in.

Geen automatische verlenging

Het lijkt mijn ten enen male juridisch onmogelijk als VZVZ stilzwijgend een gebruiksovereenkomst die plotseling een aantal wezenlijk gewijzigde artikelen bevat een eerdere minder vergaande versie doet laten vervangen. Het komt mij voor dat de gebruikers, zijnde de aangesloten zorgaanbieders, opnieuw en wel voorgelicht het contract ter tekening aangeboden krijgen. Het is te hopen dat de reeds aangesloten zorgaanbieders/zorginstellingen ook zeer kritisch kijken naar de nieuwe gebruiksovereenkomst en hun deelname een VZVZ heroverwegen.

W.J. Jongejan

Blauwdruk over cybersecurity bij ziekenhuizen. Een heldere analyse uit de VS



[Op 23 januari 2016 publiceerde het Amerikaanse bedrijf Independent Security Evaluators \(IDE\)](#) een studie op basis van eigen research over de cybersecurity in de zorg, met name ten aanzien van ziekenhuizen. De titel is "Securing Hospitals". Over dit onderwerp publiceerde ik reeds eerder [op 1 februari j.l.](#) en [op 18 februari](#). Het is een kwestie waarvan je op voorhand zou zeggen dat in die sector de computerveiligheid goed geborgd zou moeten zijn, maar niets is minder waar. Regelmatig verschijnen er in de internationale pers berichten over gehackte ziekenhuizen of andere gezondheidszorginstellingen. Het varieert van alleen het aantonen dat hackers in de systemen binnen zijn geweest tot het plaatsen van ransomware. Daarbij versleutelt de malicieuze software van de hacker de programmatuur en data en geeft die pas vrij na betaling van "losgeld". Zoals ik in beide artikelen al verwoordde is er ten aanzien van de cybersecurity in de zorg nog veel te doen. Natuurlijk kan men stellen dat zaken in Nederland anders geregeld zijn dan in de Verenigde Staten, maar de basis van de problematiek is overal hetzelfde.

Onderzoek

Van januari 2014 tot januari 2016 deden wetenschappers, die verbonden zijn aan [IDE](#) onderzoek naar de cybersecurity in

twalf zorginstellingen(voornamelijk ziekenhuizen), twee data-opslagfaciliteiten voor de zorg, twee gecomputeriseerde medisch-diagnostische apparaten en twee webapplicaties. Men nam aan dat hackers en criminelen makkelijk aanvallen ertegen konden lanceren en de gezondheid van de patiënt in gevaar brengen. Binnen die instellingen en bij de fabrikanten van medische apparatuur werd uitgebreid geanalyseerd waar de zwakke plekken in de beveiliging zaten. Ook werd gekeken met "besmette" USB-sticks die met opzet bijv. op het parkeerterrein van de instellingen achter gelaten werden, waar de kwetsbaarheden in de systemen zitten. In de ziekenhuizen werden alle geledingen van die instellingen onder de loep genomen om die uitgebreide analyse te maken. Aan de hand van die analyse werd een uitgebreide blauwdruk gemaakt. Die blauwdruk is een actieplan aan de hand waarvan stapsgewijs het veiligheidsbewustzijn wordt opgevoerd en oplossingen dan wel oplossingsrichtingen worden gegeven voor geconstateerde gebreken.

Rapport

Het 71 pagina's tellende rapport is van de eerste tot de laatste letter uitermate boeiende materie. Grafisch wordt een gedetailleerd aanvalsmodel gepresenteerd in de vorm van een cirkelvormige afbeelding waarin de gehospitaliseerde patiënt centraal staat. De relaties met relevante onderdelen van een ziekenhuisorganisatie worden door middel van sectoren aangegeven. Per sector worden de kwetsbaarheden benoemd en oplossingsrichtingen aangedragen.

Resultaten

In de ziekenhuiswereld is het tamelijk slecht gesteld met de veiligheid van de elektronische systemen door:

- het ontbreken van uitvoerende ondersteuning,
- onvoldoende gekwalificeerd personeel
- onjuiste implementatie van de technologie

- achterhaalde begrip van wat de tegenstander, hacker of crimineel, vermag
- gebrek aan leiderschap,
- een misplaatste vertrouwen op de naleving van regels en procedures

Deze bevindingen bewezen de grote angst van de onderzoekers, te weten: de gezondheid van de patiënt blijkt uitermate kwetsbaar in zorginstellingen door potentiële uitval dan wel malfunctie van elektronische systemen.

Aanrader

Het rapport is een absolute aanrader voor iedereen die in de zorg werkt. Niet alleen het ICT-personeel, maar ook artsen en verpleegkundigen doen er goed aan hun horizon te verbreden. Een groter veiligheidsbewustzijn in zorginstellingen ten aanzien van computers en aan computers gekoppelde apparatuur is geen luxe.

Het is allemaal nodig om dat te doen wat zorgverleners graag willen: goede zorg voor de patiënt.

W.J. Jongejan

**Verbieden Whatsapp bij artsen
klein bier voor in grote
privacy-zaken stille
Autoriteit Persoonsgegevens**



Al enige tijd, maar vooral na de jaarwisseling, laat de Autoriteit Persoonsgegevens (AP), voorheen het College bescherming Persoonsgegevens (CBP), van zich horen door het doen van ferme uitspraken. Het gaat dan bijna altijd om privacy-gaan, die op de keper beschouwd als “klein bier” te beschouwen zijn. Zo ging het in januari 2016 ook over camera's in sauna's. en in vrachtwagencabines. Grote privacy-zaken worden mondjesmaat aangepakt. Privacy-zaken die de samenleving op dit moment sterk bezig houden, zoals de schendingen van privacy in de jeugdzorg en rond de Suwinet-problematiek krijgen nauwelijks aandacht. Doorzettingsmacht toont de AP daarin nauwelijks. Vaak wordt eerder aangestuurd op nieuwe wetgeving om privacy-gaten te dichten dan dat de AP er uitspraken over doet.

Whatsapp

De aanleiding voor het schrijven van dit artikel is [de ruime aandacht in de media](#) die het verbieden van [het gebruik van WhatsApp door artsen](#) kreeg. De AP meldt op [de website van Medisch Contact](#) zelfs dat een individuele arts een bestuurlijke boete opgelegd kan krijgen als de privacy van een patiënt geschonden is. Krachtige taal, maar uit de AP zich altijd op diezelfde wijze bij andere zaken? Laat de AP de tanden wel echt zien bij grote schendingen van de privacy? Helaas moet aan de hand van enkele voorbeelden vastgesteld worden dat die fermheid toch heel beperkt is en vrijwel nooit getoond wordt als het gaat door privacy-overtredingen door de lokale of hogere overheden.

Undermanned/Understaffed

De privacy-waakhond is door de politiek met financiële middelen fors genuilkorfd. In het afscheidsinterview in de NRC van de voormalige voorzitter van het CBP, Jacob Kohnstamm, gaf hij aan dat een vervijfvoudiging van het budget nodig was om het CBP, Nu AP, naar behoren de taken te laten verrichten. Er kwam geen budgetverruiming, waardoor de AP zelf aangeeft per jaar maar 15 tot 20 grote zaken te doen. Het is daarbij ook maar de vraag wat onder groot verstaan wordt.

Jeugdzorg-1

Bij de grote veranderingen in de zorg speelt ook de overheveling van de jeugdzorg richting gemeenten wat betreft het uitvoeren en de financiering. [Inmiddels is het wijd en zijd bekend dat binnen de gemeenten teveel mensen, meestal zonder medische beroepsgeheim weet hebben van de meest gevoelige details van cliënten.](#) Gegevens worden gecommuniceerd over onbeveiligde verbindingen. Het meest stuitende is dat de ouders van cliënten onder druk worden gezet bij de huisarts het volledige medische dossier uitgeprint op te vragen en te overhandigen aan niet aan enig beroepsgeheim gebonden gemeenteambtenaren. Bij bezwaren krijgt men te horen dat er anders niet over de casus beslist kan worden. Horen we hier de AP krachtig over oordelen en gemeenten openlijk dreigen met boetes? Neen.

Jeugdwet-2

Op dit moment is er een veegwet voor de jeugdzorg in de maak, wetsontwerp 34111. In de eerder van kracht geworden [Jeugdwet staat in artikel 7.4](#) dat de Colleges van burgemeester en wethouders van gemeenten verplicht zijn om incidenteel dan wel systematisch informatie verkregen in het kader van de jeugdhulpverlening door te leveren aan de ministers van Volksgezondheid, Welzijn en Sport en aan die van Veiligheid en Justitie. Het is bedoeld voor het gebruik bij beleidsontwikkeling, maar kan onvoorzien toch een eigen leven gaan lijden. Over dat soort onderwerpen spreekt de AP bij het

maken van de genoemde veegwet af en toe mee, maar er wordt naar buiten toe geen duidelijk signaal over afgegeven. Daardoor is alles niet bepaald transparant.

Suwinet

Dit is [de koppeling van diverse grote overheidsbronbestanden](#) waardoor veel data van een burger in één klap opgevraagd kunnen worden. Het is opgezet in het kader van de wet Syri, afkorting van Systeem Risico Indicatie. [Jacob Kohnstamm noemde het als voorzitter van het CBP zelfs een regelrechte ramp](#). Recent bleek dat van een [steekproef bij dertien gemeenten slechts bij twee](#) de protocollen en hantering op orde waren. De AP schetste bij het publiceren van het onderzoek toch nog een rooskleurig beeld. Er viel niets te bespeuren van bestuurlijke dwang, geen dreigement met boetes. Eerst gaat men de betrokken gemeenten weer wat maanden volgen en daarna beslist men weer verder.

LSP

Ook bij het Landelijk SchakelPunt(LSP) is er niet sprake van spraakmakende acties. Bij de start werd een beoordeling van het doorstartmodel gegeven dat positief was, maar het toenmalige CBP stelde toen zelfs al dat zulks niets zei over het daadwerkelijke functioneren. Een beoordeling van de praktijk daarvan heeft tot heden niet plaatsgevonden. Een onderzoek over het geven van opt-in-toestemmingen leverde een flink aantal manco's op. Het CBP koos niet voor het gelijk publiceren van die manco's en krachtige taal uitslaan, maar liet de beheerder van het LSP, VZVZ eerst weerwoord EN correctie van gemaakt fouten toe, alvorens een gematigd oordeel publiek te maken.

Brede borst

De Autoriteit Persoonsgegevens wekt de indruk vooral een ferme indruk te wekken in kleinere privacy-zaken die niet direct overheden betreffen. Waar het overheden betreft is er dan geen

ferme standpuntbepaling, maar vaak een sturende beweging naar een in de ogen van de AP redelijke oplossing. Daarbij wordt ook nog weleens een signaal richting politiek afgegeven om het gemelde probleem door weer nieuwe wetgeving op te lossen.

W.J. Jongejan

CEO Philips bemoeit zich medische datacommunicatiewet in Eerste Kamer



[In het dagblad de Telegraaf van vandaag](#) staat een opvallend artikel over uitspraken van de CEO Frans van Houten over het wetsontwerp 33509 over de medische datacommunicatie. De behandeling ervan sleept zich in Eerste Kamer, omdat de minister van VWS voor een nogal discutabele inhoud ervan zorgde. Van Houten deed die uitspraken in de aanloop naar een grote conferentie over ICT in de zorg in [Las Vegas, van 29 februari tot en met 4 maart in, de HIMMS.](#)

Dit is de jaarlijkse conferentie van de Healthcare Information and Management Systems Society in de Verenigde Staten. Onder de kop: "Philips wil meer openheid patiëntinformatie" zegt van Houten dat zorgverleners makkelijke toegang moeten krijgen tot die informatie. Hij spreekt de hoop uit dat de Eerste Kamer het wetsontwerp 33509 aanneemt. Het is niet van eigen belang van Philips ontbloot.

Bezorgd

Toch is hij bezorgd over de afloop van de behandeling, want hij vermeldt dat bezorgdheid over privacy deze wet zou kunnen tegenhouden. Hij acht het wel oplosbaar en stelt dat deze problematiek goede zorg niet in de weg mag staan. Het echter zo dat in de Eerste Kamer, maar ook daarbuiten grote zorg bestaat over de privacy ten aanzien van medische gegevens van burgers als deze wet aangenomen wordt. Tussen de regels door geeft hij eigenlijk aan dat privacy de "vooruitgang" in de weg staat. De wet gaat in naam om alle vormen van medische datacommunicatie, maar is eigenlijk volledig geschreven om de het gebruik van het Landelijk SchakelPunt(LSP) voor die communicatie een wettelijke basis te geven. Er bestaan fundamentele bezwaren bij een groot aantal partijen in de Eerste Kamer over hoe één en ander door het ministerie van VWS in het wetsontwerp voorgesteld wordt.

Vergelijking

Van Houten komt nog met een vergelijking met het bankwezen en wijst op het internetbankieren. Het probleem is echter dat financiële informatie, hoewel die ook zeer gevoelig is, niet met medische informatie te vergelijken is. Medische data zijn bij een te grote openheid van een andere orde dan geldzaken. Er is nog een verschil: bij het internetbankieren hebben mensen zélf een pas. Het LSP doet het anders: naar analogie van dat model heeft de patiënt zelf geen PIN-pas maar vertrouwt hij/zij iedere bankmedewerker, die een pasje heeft

en die zegt dat hij een bankier of bankmedewerker is, om voor u geld te pinnen. Dat wil de burger voor geld ook niet, laat staan voor medische data...

Resource-grabbing

De woorden van de topman van Philips zijn absoluut niet van eigenbelang voor zijn bedrijf ontbloot. Gemakkelijke beschikbaarheid van medische data is gezien de koers de Philips vaart geen vreemd oogmerk. Philips zet namelijk hoog in op het ontsluiten van big-data, het analyseren ervan en op basis daarvan producten in de markt zetten. Philips zet daarbij in op cloud-based data-analyse. De keuze wordt [door het online Zorg-ICT-magazine als opvallend](#) bestempeld. Dat is echter in geen dele het geval. Grote internationaal opererende bedrijven hebben dondersgoed door dat het gebruik en analyseren van big-data het nieuwe goud is. "Data-grabbing" is de nieuwste vorm van "resource-grabbing" die we in [allerlei tijdperken in de geschiedenis gekend hebben](#). Telkenmale wordt gesteld dat de onderliggende data of geanonimiseerd of gepseudonimiseerd zijn, maar helaas blijkt maar al te vaak dat met ICT-inspanningen toch te herleiden zijn tot mensen van vlees en bloed.

Philips heeft een samenwerkingsverband met de verzekeraar Allianz uit Duitsland. Op basis van die samenwerking bespaart Allianz geld volgens Philips, omdat verzekerden meedoen met levensstijl- en rugklachtenprogramma's en zo gezondheidswinst boeken. Philips registreert met sensoren de lichaamsfuncties en analyseert die in de cloud. Waarschijnlijk krijgen de bij Allianz verzekerden op basis van hun medewerking korting op hun verzekeringen. Het doet een beetje denken aan het autorijden met een registratiekastje voor het rijgedrag waarbij verzekerden dan korting op de premiekrijgen. De vraag is bij dit alles of dit soort ontwikkelingen wel echt wenselijk zijn.

Opvallend

Verbazingwekkend is dat van Houten in de Telegraaf de hoop uitspreekt dat de Eerste Kamer de wet aanneemt, waardoor de patiënt niet meer per zorgverlener maar per categorie van zorgverlener goedkeuring kan geven om informatie te delen. In de voorliggende wet 33509 is nooit sprake geweest van het geven van goedkeuring per zorgverlener, maar werd voorgesteld om het per categorie te doen middels een systeem van het aan- en uitzetten van zorgverleners-categorieën. In de laatste verwickelingen rond het wetsontwerp wil de minister van VWS dat aan- en uitzetten juist drie jaar uitstellen vanwege uitvoeringsproblematiek. Correcte uitwisseling van medische gegevens met behoud van privacy geschiedt alleen, wanneer bepaald kan worden, welke (beperkte) informatie voor een specifiek gekend doel mag worden verstrekt aan een gekende derde. Dat kan bijv. met [de Whitebox](#), maar niet met het LSP. Van Houten toont zich met zijn uitspraken wel heel erg duidelijk een voorstander van het wijd opstellen van medische dossiers.

De uitspraak van de topman van Philips acht ik in het debat rond het wetsontwerp geen verstandige.

W.J. Jongejan

22-02-2016 Aanvulling alinea Vergelijking WJJ

**VZVZ produceert inhoudsloos
nieuws over aansluitingen**

ziekenhuizen op LSP



Op 16 februari 2016 j.l. kwam de Vereniging van Zorgaanbieders Voor Zorgcommunicatie(VZVZ) met het ronkende nieuws dat 84% van de ziekenhuizen op het Landelijk SchakelPunt(LSP) aangesloten zijn. VZVZ had na een stille periode op PR-gebied blijkbaar behoefte om goed nieuws te brengen. Wat men meldt, heeft echter nauwelijks inhoud. Al enige tijd lag het percentage boven de 50% . Waarom die 84 % nu opeens nieuws is, is een raadsel. Dat het weinig zegt heeft te maken met het feit dat aangesloten zijn en gebruik maken het LSP twee volkomen verschillende zaken zijn. Aan de hand van de gegevens over de huisartsen is daar duidelijkheid over te verschaffen.

Huisartsen

[Volgens de informatie op de website van VZVZ](#) is 90 % van de huisartsen aangesloten op het LSP. Nu doet er zich een op het oog vreemd fenomeen voor. Er blijkt gemiddeld slechts 30% van de Nederlanders de opt-in-toestemming gegeven hebben voor het beschikbaar stellen van hun huisartsgegevens voor inzage door andere zorgaanbieders. Bij de apothekers is dat percentage het dubbele ervan. Blijkbaar laat men makkelijker medicatiegegevens inzichtelijk dan huisartsgegevens. Er kunnen ook daadwerkelijk weinig huisartsgegevens ingezien worden. Daarnaast is het zo dat in het recente verleden een subsidieregeling heeft bestaan voor huisartsen om aan te sluiten op het LSP. Daardoor gelokt hebben meerdere huisartsen zich laten aansluiten, maar hebben bij nader inzien er verder

niets mee gedaan. Ook speelt mee dat in sommige regio's, zoals bijv. in Groningen de software op de huisartsenpost (ADASTRA in Groningen) gewoon nog steeds niet overweg kan met het berichtenverkeer via het LSP. Er zijn nog steeds regio's waar het aantal opt-in-toestemmingen beneden de 10% ligt. Het moge duidelijk zijn aan de hand van deze voorbeelden dat het percentage aansluitingen totaal niets zegt over het daadwerkelijke gebruik.

NVZ

VZVZ meldt in het bericht dat een trotse externe projectleider van de Nederlandse Vereniging

van Ziekenhuizen (NVZ), [Erwin van Malland, verslag doet](#) over de ervaringen van zes ziekenhuizen die aangesloten zijn op het LSP. Zowel in het bericht van VZVZ als van de NVZ staan echter geen getallen over het daadwerkelijke gebruik van het LSP.

Overigens moet de patiënt in het ziekenhuis ook aan de ziekenhuisapotheek een opt-in-toestemming geven om daar de gegevens met anderen via het LSP te doen delen als de ziekenhuisapotheek er al toe in staat is (woorden projectleider). Specialisten kunnen zelf geen informatie beschikbaar stellen. Zodra dat zou kunnen, moet de patiënt ook daar een opt-in-toestemming geven.

Nauwkeurigheid

Wat kan er nu worden opgevraagd door specialisten in ziekenhuizen en hoe nauwkeurig is die informatie? Het enige wat de specialisten binnen ziekenhuizen [nu kunnen opvragen zijn de medicatiegegevens](#). Het gaat om medicatie plus de interacties, contra-indicaties en allergieën. Die zijn niet altijd correct en in overeenstemming met wat in het ziekenhuis bekend is.

Zie wat de projectleider daar over zegt:

Doseringen die verschillen tussen tweede en eerste lijn over en weer kunnen vertalen. In de ziekenhuissystemen moeten daarvoor omrekenstabellen worden aangevuld met de doseerschema's uit de eerste lijn. Doordat nu doseringen van één en hetzelfde geneesmiddel in tweede en eerste lijn verschillen, zal een apothekersassistent – voordat de regel wordt verwerkt – de dosering moeten beoordelen. Er zullen altijd verschillen blijven bestaan maar nu is het aantal te groot en kost dat te veel tijd.

Het probleem is dat patiënten na opnamen en polikliniekbezoek medicatie voorgeschreven krijgen door een specialist. Bij thuiskomst blijkt dan dat de specialist iets voorschreef wat de patiënt onder een andere naam al kreeg of dat de dosering na enkele dagen te hoog of te laag bleek te zijn, waardoor op gezag van de huisarts aanpassingen zijn gemaakt in de dosering die de apotheek niet gemeld zijn.

Dat is een probleem dat vrijwel onuitroeibaar is. Zowel [NHG](#) als [VZVZ](#) zijn bezig met een project om de medicatieafspraken en het verstrekkingsverzoek aan de apotheek van elkaar te scheiden. Het is een illusie om te denken dat zo iets snel te regelen, los van de vraag of dit proces wel op deze manier het probleem aan de ziekenhuiskant oplost. Nu wordt dus door een apothekersassistent in het ziekenhuis de dosering weer handmatig gecontroleerd plus dat verificatie bij de patiënt noodzakelijk is.

Gebakken lucht

Uit het voorgaande moge duidelijk zijn dat het bericht van VZVZ eigenlijk vooral gebakken lucht bevat en eigenlijk alleen bedoeld is om positief nieuws de wereld in te brengen. Wat men aan percentage aansluitingen brengt, zegt totaal niets over het daadwerkelijke gebruik van het LSP.

Het is daardoor in de rubriek juichtaal en mooipraat te onder te brengen.

Cybersecurity in medische sector: Witte Huis geeft goed voorbeeld



Terwijl enerzijds diverse veiligheidsdiensten in de Verenigde Staten koplopers zijn in het elektronisch afluisteren en volgen van burgers, is daar anderzijds ook een groeiend besef van de kwetsbaarheid van medische apparatuur en hulpmiddelen die aan elektronische ziekenhuisnetwerken gekoppeld zijn. [Zeer recent, in januari 2016 werd op initiatief van het Witte Huis, aldaar een ronde tafelgesprek gehouden](#) over cybersecurity in ziekenhuizen en rond elektronische medische apparaten. Eén van de deelnemers, Kevin Fu, professor aan de universiteit van of Michigan en leider van het Archimedes Center for Medical Device Security, bericht hierover op zijn blog. Kevin Fu was [ook spreker op de Enigma 2016 conferentie waarover ik recent berichtte in het kader van het risicobewustzijn](#) bij zorgaanbieders ten aanzien van elektronische medische apparatuur. Op die bijeenkomst waren naast vertegenwoordigers van de fabrikanten van deze apparatuur ook veiligheidsexperts uit het bedrijfsleven, van overheidsinstanties (waaronder de FBI) en universiteiten aanwezig om te brainstormen over dit

onderwerp.

Bijeenkomst

De deelnemers waren bijeen geroepen door de [President's Office of Science and Technology Policy \(OSTP\)](#) en werd geleid door een tweetal cybersecurity experts van het Witte Huis. Tijdens de sessie werd gesproken over regelgeving door diverse overheids- en gezondheidszorgorganisaties, over bestaande risico's met medische elektronica, over hoe bewust fabrikanten zich zijn van de inbraak- en beïnvloedingsrisico's van de producten die zij maken en met welke inspanningen dat voorkomen kan worden. Professor Kevin Fu was daar vanwege zijn expertise betreffende de veiligheidsissues rond medische elektronische apparatuur en de regelgeving van de Food and Drugs Administration op dat vlak. Bovendien had hij in de jaren 90 van de vorige eeuw in de ziekenhuis ICT-gewerkt en op de werkvloer gezien waar de risico's zich bevinden.

Kevin Fu

Professor Fu sprak op de bijeenkomst desgevraagd over de cybersecurity in ziekenhuizen, over de fabrikanten van elektronische medische apparatuur, over het waarom van de problemen en hoe de diverse stakeholders omgaan met de problemen. Hij vertelde dat het goede nieuws was dat de fabrikanten en ziekenhuizen tegenwoordig serieus geïnteresseerd zijn en naar wegen zoeken de cybersecurity-risico's te beperken. Daarnaast benadrukte hij dat het grootste gevaar op dit moment niet veroorzaakt wordt door high-tech inbraken, maar door niet al te nieuwe huis-tuin- en keuken-malware. Het veroorzaakt tijdelijke uitval van de aangedane systemen vanwege het opruimen van de narigheid en de systemen weer draaiend te krijgen. De verstoring van de patiëntenzorg is dan het grootste probleem. Hij had daar uitgebreid over gepubliceerd o.a. in een artikel in de [National Academy of Engineering Winter 2015 newsletter](#) en in

2011 in een verslag van een workshop op het [Institute of Medicine](#) van de universiteit van Michigan.

Cultuur

Waar hij sterk de nadruk op legde was het belang van het begrijpen van de arbeidscultuur in de ziekenhuizen en andere gezondheidszorginstellingen. Alle extra ballast die ziekenhuisautomatisering voor de artsen en verpleegkundigen met zich mee brengt, wordt door dezen als hinderlijk ervaren tijdens het werk. Het gevolg is dat iedereen workarounds gaat bedenken om zo min mogelijk last te hebben van de eisen van ICT-ers. Hij hield daarom ook de ICT-mensen een devies voor: "thou shalt not interrupt clinical workflow! Period!". Let men niet op het verstoren van de dagelijkse routine in ziekenhuizen dan kan met succes met de ICT-plannen wel vergeten. De dokter/verpleegkundige wil de patiënten behandelen en zo min mogelijk last hebben van hinderlijke ICT-zaken. Fu geeft hiermee aan de problemen van de werkvloer even goed te begrijpen als de problemen van het management en de overheid met de cybersecurity.

Samenwerking

Professor Fu hield ook een krachtig pleidooi richting mede-wetenschappers om uit hun ivoren torens op de universiteit te komen en met de instanties die zich met de cybersecurity bezighouden te werken aan het verminderen van de risico's. Veel stilzitten is er niet meer bij want in de week voordat Kevin Fu zijn blog schreef (31-01-2016) waren er drie ziekenhuizen door cybersecurity-problemen in de narigheid verdaagd. [[a](#), [b](#), [c](#)]. Ook blijken er nu fabrikanten te zijn die nog steeds moeilijk te beveiligen elektronische medische apparatuur maken ([remote buffer overflows in drug infusion pumps](#))

Nederland

De les die uit dit blog en de bijeenkomst waarover die ging in

het Witte Huis getrokken kan worden is dat een overheid op goede gronden een samenwerkingsproces kan brengen van werkers in de gezondheidszorg, wetenschappers, fabrikanten en overheidsinstanties om cybersecurity-risico's tot een aanvaardbaar minimum te beperken. Volledig naar nul terugbrengen is een utopie. De inzet van allen moet niet éénmalig zijn maar er moet sprake zijn van een permanent proces.

Nederland is elektronisch gezien als het ware de proeftuin van Amerika. Wij scoren met de dichtheid van internet-aansluitingen en computer diensten zeer hoog. Het is een illusie om te denken dat de beschreven problemen hier niet voorkomen. Het volstaat niet met het roepen van ach en wee bij het hacken van ziekenhuizen of dataverlies door criminele oorzaken. Het zou verstandig zijn als de Nederlandse overheid op dezelfde wijze als het Witte Huis de (knappe) koppen bij elkaar zou laten steken in samenwerking met de andere stakeholders op het vlak van cybersecurity in ziekenhuizen en met medische apparaten. In Nederland bestaat sinds 1 januari 2012 het Nationaal CyberSecurity Security Centrum(NCSC), maar het is mij niet duidelijk of het NCSC zich met de hierboven beschreven problematiek zich bezig houdt.

Nog even een aardige anekdote op dit vlak: oud-vice-president Dick Cheney die te boek staat als een "havik" kreeg in 2007 een pacemaker met ingebouwde defibrilaator(ICD) i.v.m. vrij grote hartproblemen. Hij heeft de mogelijkheid om de pacemaker "wireless" te benaderen uit laten zetten omdat hij bang was, op basis van wat wetenschappelijke berichten, dat de pacemaker op afstand door terroristen uitgezet kon worden of kwalijke acties ging uitvoeren

W.J. Jongejan

Petitie verontruste burger om medische datacommunicatie via het LSP te doen stoppen



Vandaag werd ik attent gemaakt op een [burgerinitiatief in de vorm van een petitie](#) via het internet met als doel de elektronische uitwisseling van medische gegevens via het Landelijk SchakelPunt(LSP) te doen stoppen. Mevrouw J. Berkelaar, de initiatiefneemster, spreekt in der petitie haar verontrusting uit over het LSP. Naast de petitietekst is er ook [een onderliggend opiniestuk beschikbaar](#) waarin ze dieper ingaat op de materie. Via de petitiewebsite is dat stuk ook benaderbaar.

Het aardige van deze petitie is dat deze nu niet een keer uit de medische hoek zelf komt maar door een verontruste burger is opgesteld. Niet door iemand die gelieerd is aan de Vereniging Praktijkhoudende Huisartsen(VPHuisartsen), die via de rechter het LSP-gebruik probeert te beëindigen. Het vonnis van het hoger beroep in de zaak van VPHuisartsen tegen VZVZ(vereniging van Zorgaanbieders Voor Zorgcommunicatie) zal overigens eind deze maand of uiterlijk eind maart 2016 uitgesproken worden.

Blijkens het opiniestuk dat mevrouw Berkelaar schreef is zij goed op de hoogte van de ins en outs van de bezwaren tegen het

LSP, die geuit zijn door de tot nu toe opgestane tegenstanders van het LSP.

De gemiddelde burger heeft nauwelijks weet wat er met zijn/haar medische data gebeurt bij communicatie via het LSP. Vaak wordt de burger alleen maar gevraagd of de huisarts op de huisartsenpost de medische data bij de eigen huisarts mag inzien, of gevraagd door de apotheker of die de medicatiehistorie in het huisartsdossier mag inzien. Men weet vaak niet dat zulks via een centrale landelijke computer gaat, genaamd het LSP.

Dat vanuit deze hoek nu dit initiatief komt is een positieve ontwikkeling.

W.J. Jongejan

Autoriteit Persoonsgegevens maant besturen zorginstellingen om onterechte dossier-inzagen



[Op 15 februari 2016 vraagt de Autoriteit Persoonsgegevens\(AP\)](#)

[in een open brief](#) aan De Raden van Bestuur van zorginstellingen(ziekenhuizen, huisartsenposten, GGz) in Nederland om aandacht voor de bescherming van persoonsgegevens. [De AP schrijft op haar website](#) dat zij regelmatig vragen en signalen krijgt over patiëntendossiers, die onder ogen zouden zijn gekomen van medewerkers van zorginstellingen, die daar niets mee te maken hadden. Een zorginstelling moet bij de verwerking van persoonsgegevens voldoen aan de vereisten van de Wet bescherming persoonsgegevens(Wbp) en kan patiënten niet aan het risico blootstellen dat onbevoegden medische gegevens inzien(woorden AP, WJJ)

Onvoldoende inspanning

[Eerder onderzoek\(2013\)](#) had laten zien dat zorginstellingen zich onvoldoende inspannen om te voorkomen dat mensen die niet bij de behandeling betrokken zijn inzage hebben in digitale medische dossiers. Vanwege de privacy-gevoeligheid en het overtreden van artikel 13 van de Wbp maant de AP de Raden van Bestuur van zorginstellingen erop toe te zien dat er voldoende aandacht is voor deze materie en dat men maatregelen neemt om zaken op orde te brengen. De AP verwacht een leidende rol van de Raden van Bestuur hierin. Daarbij wijst de AP enerzijds op reputatieschade voor de instellingen bij overtredingen, maar ook op de kans dat bij voortdurende onzorgvuldigheid de patiënt het vertrouwen in de zorgaanbieders verliest. Dat kan dan patiënten afschrikken om tijdig zorg te vragen.

Gebreken

De gebreken die in 2013 zijn vastgesteld gingen om:

- Te ruime autorisaties aan medewerkers voor de toegang tot de digitale medische dossiers
- Het ontbrak vaak aan controle van die toegangsrechten, waardoor ondanks het soms aanwezig zijn van een sanctiebeleid toch in de praktijk geen sancties

ingesteld werden bij overtredingen

Maatregelen

De AP wil dat er sprake is van:

- Correcte afbakening van de autorisaties van het personeel.
- Een beperking in de tijd voor toegang tot het elektronische dossier, voorafgaand en na beëindiging van het contact met de patiënt.
- Logging van het inzien van een dossier
- Stelselmatige daadwerkelijke controle van de logging
- Optreden door sancties bij overtredingen.

Tanden

Met de genoemde publicaties van de AP laat deze nu een keer een klein beetje zien dat men tanden heeft. Hoewel het nergens zo genoemd staat, zou het onbevoegd inzien van digitale medische dossiers als een door een instelling toegelaten intern mini-datalek beschouwd kunnen worden. Datalekken dienen sinds 1 januari 2016 aan de AP gemeld te worden en kunnen eventueel bij onvoldoende beveiliging bestraft worden. Met een beetje goede wil is een intern datalek ook zo door de AP te bestraffen.

W.J. Jongejan

Opgevraagde informatie via LSP bij Medicom doordeweeks niet direct compleet



Uit doorgaans goed ingelichte bron vernam ik, dat teveel bevestigingen via het Landelijk SchakelPunt(LSP) momenteel tot overbelasting kunnen leiden van de centrale servers van het huisartsinformatiesysteem(HIS) Medicom. Die overbelasting kan dat HIS trager doen werken en de communicatie via het LSP doen uitvallen. Om dit tegen te gaan wordt de komende tijd de verse informatie, die een huisarts vastlegt in zijn elektronische dossier pas 's-avonds beschikbaar gesteld voor bevestiging via het LSP. Het betekent dat als de patiënt voor dat tijdstip een andere arts bezoekt bij opvraging de data niet volledig kunnen zijn. Door Medicom wordt een soort workaroud voorgesteld. Er wordt gewerkt aan een upgrade van de LSP-omgeving om dit probleem uit de wereld te helpen, maar absoluut geen termijn genoemd in de informatie die de gebruikers toegestuurd kregen.. Tot die tijd is het dus behelpen.

Servers

Pharmapartners, de producent van Medicom, heeft de servers voor het onder ASP(Application Server Provider) draaiende HIS staan in het KPN CyberCentrum Flevoland te Almere. Als een patiënt de opt-in-toestemming voor het bevragen van zijn medische dossier via het LSP heeft gegeven wordt informatie daaruit (in de vorm van de Professionele Samenvatting)

beschikbaar gemeld aan het LSP. Als de patiënt op het spreekuur is geweest wordt op de achtergrond automatisch aan het LSP gemeld dat het dossier gewijzigd/aangevuld is. Deze meldingen veroorzaken de huidige overbelasting. Als oplossing heeft men bedacht dat de wijzigingsmeldingen doordeweeks pas tussen 17.00 en 20.00u uitgevoerd worden. In de weekenden en in de avonden gebeurt het iedere vijf minuten. Dat kon ook haast niet anders omdat in deze perioden de kans op een hernieuwd contact met de huisarts bij spoedgevallen of ernstige ziekten vrij groot is. Het uitstellen van de wijzigingsmelding gebeurt niet bij dossiers van patiënten die nog niet eerder bij het LSP bekend waren en waarvan voor het eerst na hun opt-in-toestemming gemeld wordt aan het LSP dat gegevens beschikbaar zijn voor bevraging.

Gevolgen

Medicom werkt met clusters van huisartsen en apotheken. Binnen een cluster communiceert men met elkaar zonder het LSP. De gegevens zijn dan altijd up to date. Als een patiënt in de ochtend naar een huisarts of apotheker gaat die met Medicom werkt en hij gaat in de middag naar een zorgaanbieder met Medicom buiten het cluster of naar een zorgaanbieder met een ander HIS, dan mist die bij het inzien via het LSP de informatie die in de ochtend is ingevoerd. Bij handmatige bevraging via het LSP wordt de ontbrekende informatie WEL opgehaald.

Het advies aan de huisartsen en apothekers, die met Medicom werken is, om aan de patiënt te vragen of die eerder op de dag nog bij een andere zorgverlener is geweest of medicatie voorgeschreven heeft gekregen. Is de patiënt of zijn omgeving niet in staat om daar iets over te melden dan krijgt de zorgaanbieder het advies van PharmaPartners om dan altijd handmatig het LSP te bevragen.

Incompleet

Het moge duidelijk zijn dat doordeweeks de informatie die bij een Medicom-zorgaanbieder(huisarts of apotheker) via het LSP automatisch wordt opgevraagd incompleet kan zijn. Het kan nooit de bedoeling zijn geweest van een systeem als het LSP dat handmatig geverifieerd moet gaan worden of de getoonde informatie die verkregen is via het LSP wel compleet is. Het is juridisch ook een interessante zaak hoe het ligt met de verantwoordelijkheid voor de gevolgen van het incompleet zijn van informatie in deze casus. De HIS-leverancier verlegt namelijk de verantwoordelijkheid voor het krijgen van de meest recente informatie naar de opvragende zorgaanbieder. Deze zou er echter vanuit moeten kunnen gaan dat er geen extra handelingen nodig zijn om de informatie compleet te maken.

Het betekent weer hoe de performance van het LSP verzwakt door een zwakke schakel aan de kant van de huisartsinformatiesystemen.

W.J. Jongejan

**Het is stil aan de overkant.
VZVZ en ZN stil voor
uitspraak Hof**



Bij voetbalwedstrijden komt het nog wel eens voor dat er door supporters,

als de aanhangers van de tegenstanders zich nauwelijks roeren, op de tribunes gezongen wordt: "Het is stil aan de overkant". Het zelfde kan nu gezegd worden van Zorgverzekeraars Nederland(ZN) en de Vereniging voor Zorgaanbieders Voor Zorgcommunicatie(VZVZ) in afwachting van de uitspraak van het gerechtshof in Arnhem. Daar diende op 11 december 2015 het hoger beroep in de zaak van de Vereniging Praktijkhoudende Huisartsen (VPHuisartsen) tegen VZVZ over het Landelijk SchakelPunt(LSP). Ik [berichtte daar op 23 december 2015](#) over op deze website. Het is duidelijk de uitspraak van het Hof bij toewijzing van één of meerdere eisen grote consequenties kan hebben voor het functioneren en het voortbestaan van het LSP.

ZN

In het verleden, eind 2012, hebben ZN en VZVZ luid en duidelijk gecommuniceerd, dat ZN gedurende drie jaar(2013 t/m 2015) per jaar 25 miljoen euro in het in stand houden en door-ontwikkelen van het LSP zou stoppen. [Eind 2014 heeft ZN](#) haar commitment voor de jaren 2016-2020 uitgesproken, maar daarna is nimmer een persbericht met opgave van bedragen verschenen over het doorgaan van de financiële injectie in VZVZ door ZN ten behoeve van het LSP. Het uitblijven van berichtgeving hierover kan alleen maar gezien worden in samenhang met het lopende hoger beroep van VPHuisartsen tegen VZVZ. De uitspraak staat gepland op 23 februari, maar de rechters gaven ter zitting aan dat die termijn mogelijk met maximaal zes weken verlengd kan worden. Tot die tijd zal er wel geen uitspraak van ZN komen over hoeveel geld per jaar men in het LSP wil steken

VZVZ

Terwijl VZVZ in de twee maanden voor de zitting van het Hof bij herhaling op haar website aandacht vroeg voor nieuwe initiatieven, zoals het LSP willen benutten voor de gehandicaptenzorg, de caresector en voor de toegangsmogelijkheid van de spoedeisende hulp-arts is het nu al twee maanden doodstil. Bij VZVZ zal men zich ongetwijfeld afvragen hoe en waarmee men verder moet indien de eisen van VPHuisartsen geheel of gedeeltelijk worden ingewilligd bij de rechter. Dat men bang daarvoor is toonde ook het pleidooi van de advocaten bij het hoger beroep. Men vroeg

de rechters om een eventueel voor VZVZ negatief uitvallend vonnis niet bij voorraad uit doen spreken. Bij voorraad een vonnis uitspreken betekent dat hetgeen toegewezen is in het vonnis meteen na de uitspraak ingaat. Men zou dus geen schorsende werking van de uitspraak willen en bij eventuele cassatie bij de Hoge Raad gewoon met het huidige LSP door willen gaan tijdens de rechtsgang.

Dramatische terugval

Dat het allemaal minder vlot loopt met het LSP blijkt ook uit de eigen cijfers van VZVZ op de website. Terwijl in september 2015 nog gewag werd gemaakt van één geregistreerde opt-in-toestemming per zeven seconden, is dat nu drie maal zo weinig. [Op dit moment is de aanwas één per twintig seconden.](#) Een dramatische afname van de aanwas. Ook is te zien dat de stijging van de opt-in-toestemmingen veel meer bij de apotheken dan bij de huisartsen plaats vindt.

Stil

Het zal nog wel even stil blijven tot de uitspraak van het Hof er is. ZN heeft er geen enkel belang bij om ferme uitspraken te doen over verdere grootscheepse financiering van het LSP als een voor hen negatieve uitspraak mogelijk is. VZVZ zal ook nog wel ven een “low-profile” aanhouden terwijl de rechters nog aan het delibereren en formuleren zijn.

Een broedse kip moet men immers niet storen.

W.J. Jongejan