Utrecht 05-10-2020

Burgerrechtenvereniging Vrijbit

Kruisweg 32, 3513 CT Utrecht

bestuur@vrijbit.nl

Aan OpenConsultatiesInformatieBeraadzorg@minvws.nl

Onderwerp: Consultatie Mitz als online toestemmingsvoorziening

Inbreng Burgerrechtenvereniging Vrijbit op de zoveelste gezamenlijke poging van de regering en de Zorgverzekeraars Nederland om het medisch beroepsgeheim en fundamenteel burgerrecht op bescherming van het privéleven af te schaffen.

> De inbreng betreft een uitleg *met toelichting* gericht aan het ministerie van VWS op het voorstel om de fundamentele beschermingsprincipes los te laten ten aanzien van het uitwisselen van medische gegevens. En deze te vervangen door een Online ToestemmingsVoorziening(OTV).

Inleiding

Voor goede zorg is het essentieel dat patiënten erop moeten kunnen vertrouwen dat zorgverleners zich houden aan hun medisch beroepsgeheim en het recht op privacy van de patiënt respecteren. Dat betekent met betrekking tot het vastleggen en verwerken van medische gegevens dat deze in eerste instantie enkel ter beschikking horen te staan voor de patiënt zelf En voor professionele zorgverleners die direct bij een bepaalde behandeling van deze patiënt betrokken zijn waarvoor deze gegevens van belang zijn.

Voor alle overige mogelijkheden voor het gebruik van medische data geldt *dat (behoudens uitzonderlijke incidentele gevallen van gevaar)* deze gegevens uitsluitend mogen worden ingezien of uitgewisseld met zogenaamde 'derde partijen' mits de betrokken patiënt daar: 1-Goedgeïnformeerd, 2- Uitsluitend voor een welomschreven doel ,en 3- vooraf, Specifiek toestemming voor geeft.

Het betreft rechten en plichten zoals al sinds 400 v.Chr. zijn vastgelegd in de eed van Hippocrates, sinds 1814 in de Nederlandse Grondwet, sinds 1948 in de Universele Verklaring van de Rechten van de Mens, sinds 1950 in het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en sinds 2000 in het huidige Handvest van de grondrechten van de Europese Unie. DAARMEE ZIJN HET NIET ALLEEN ELEMENTAIRE FATSOENSREGELS MAAR JURIDISCH VASTGELEGDE WETTELIJKE GRONDSLAGEN WAARVAN HET VERBODEN EN DUS STRAFBAAR IS OM HIER INBREUK OP TE MAKEN. OOK VOOR DE OVERHEID WANNEER DEZE DE HAND HIERMEE WIL LICHTEN DOOR ONDER HET MOTTO VAN 'GROOT MAATSCHAPPELIJK BELANG' HIEROP INBREUK WIL MAKEN, ZOLANG DAARBIJ NIET KAN WORDEN AANGETOOND DAT DIT MAATSCHAPPELIJKE BELANG EEN CONCREET WELOMSCHREVEN DOEL BETREFT, HET EEN PROPORTIONELE MAATREGEL ZOU BETREFFEN EN DE DOELSTELLING NIET OP EEN ANDERE WIJZE GEREALISEERD ZOU KUNNEN WORDEN.

Toch gaat het om rechten waar de zorgverzekeraars in Nederland sinds 2006 voortdurend aan proberen te tornen. Gefaciliteerd overigens door de Rijksoverheid die aan deze bedrijven de regie

over de zorgsector toeschoof. Vanuit de gedachte dat de stijgende zorgkosten in de welvarende Nederlandse verzorgingsstaat bestreden dienden te worden door het invoeren van markwerking in de zorg. Waarbij als economisch principe patiënten voortaan als zorgobjecten en medische behandelingen voortaan als zorgproducten worden aangemerkt.

Sindsdien zijn deze voormalige financiële instellingen, actief jacht gaan maken op de medische diagnose-behandelgegevens en gezondheidsdata van de gehele bevolking.

Medische persoonsgegevens werden in middels namelijk veelal digitaal vastgelegd en kunnen daardoor steeds makkelijker worden uitgewisseld, geanalyseerd, gecombineerd met andere data, gebruikt worden voor het opleggen van standaardiseringsnormen m.b.t. diagnose en behandeling, voor controle en om te exploiteren voor commerciële doeleinden van onderlinge concurrentie t/m ontwikkeling van e-Health toepassingen.

Wie de beschikking heeft over de medische gegevens van de bevolking heeft daarmee goud in handen en verwerft zich een ongebreidelde informatiemacht.

> Waarbij we voor nadere toelichting op deze stelling verwijzen naar de artikelen over 'Data Grabbing in de zorg' en 'resourcegrabbing' zijnde het op grote schaal vergaren en in bezit nemen van nieuwe, nog niet toegeëigende hulpbronnen, een proces dat leidt tot een fundamentele herverdeling van de economische en bestuurlijke macht, die al in 2014 het licht zagen. Zie bijlage 1 https://www.vphuisartsen.nl/beroepsorganisaties-beseffen-onvoldoende-de-gevolgen-van-de-informatiseringsrevolutie/

Zoals gezegd, de strijd om de medische data barstte los via de zorgverzekeraars. In innige samenwerking met de overheid die zelf ook graag profiteren wil van de informatiemacht over de bevolking en maar wat graag het graag het verzamelen en aanleveren van deze data aan (nauwelijks via het bestuursrecht aan te pakken) semi-private bedrijven en organisaties overlaat.

Raadpleging voorstel invoering van het project MITZ als landelijk online toestemmingsbeheerssysteem voor uitwisseling van medische data

Onderhavige reactie betreft een inbreng op de semi-openbare raadpleging van het ministerie. Een consultatie die niet via de website van het ministerie te vinden is, maar georganiseerd wordt via het onder auspicium van VWS vallende 'Informatie Beraad'. Bron: 07-09-2020 https://www.informatieberaadzorg.nl/actueel/nieuws/2020/09/07/open-consultatie-voor-online-toestemmingsvoorziening-gestart

Een consultatie bovendien die weliswaar als 'open consultatie' wordt aangeduid maar waarvan, i.t.t. de openbare consultaties die het Rijk gewend is te organiseren, de insteek is om de reacties niet openbaar te maken maar onder de pet te houden van de indieners van het Mitz voorstel, zijnde de koepelorganisatie van de zorgverzekeraars ZN en de door de zorgverzekeraars gefinancierde beheerder van het EPD-LSP systeem VZVZ.

Bezwaren

VWS gaat met deze consultatie voort op een doodlopende weg. Ze vermijd zo om daadwerkelijk in te zetten op het ontwikkelen van systemen waarmee de uitwisseling van elektronisch vastgelegde medische gegevens op een veilige manier en met behoud van het medisch beroepsgeheim en privacy van patiënt en zorgverlener gestalte kan worden gegeven.

Toelichting

Waar er al jaren politiek getouwtrek is over de manier waarop voldaan zou moeten worden aan de vereisten qua toestemming voor het uitwisselen van medische gegevens, leek het erop dat minister Bruins eindelijk tot het inzicht was gekomen dat het hardnekkig blijven vasthouden aan het geloof dat landelijke centrale uitwisselingssystemen voor medische zorgdata een onbegaanbare weg vormde die onvermijdelijk leidt tot mislukken. Na de mislukte pogingen om een publiek EPD in te voeren, onder de ministers Klink en Schippers, zette de laatste haar kruistocht voort met het introduceren van wetsvoorstel 33-980 om buiten de toestemming van haar klanten om inzage te kunnen krijgen in hun medische data (voor controle en opsporingsdoeleinden). De Eerste Kamer ging hiermee, net als met het oorspronkelijke EPD, uiteindelijk na veel vijven en zessen niet akkoord. Waarna het voorstel werd ingetrokken al was dat met de intentie het zodanig aan te passen dat het alsnog weer ingediend zou kunnen worden. Spil in dit steekspel tussen Rijk, zorgverzekeraars en voorvechters van het behoud van medisch beroepsgeheim vormde de semantische draai van VWS om de vereisten van specifieke toestemming onder de benaming 'gespecificeerde toestemming' alsnog geaccepteerd te krijgen al ging het in de praktijk om ongeoorloofde (niet doelgebonden) generieke toestemming.

Hoewel er al jarenlang door o.a. Burgerrechtenverenigingen zoals Vrijbit, de Vereniging van Praktijkhoudende huisartsen en databeveiligingsexperts werd aangedrongen op het ontwikkelen van decentrale push (i.p.v. pull)systemen als alternatief voor de uitwisseling van medische gegevens, bleven zowel de zorgverzekeraars als het ministerie hardnekkig vasthouden aan de opzet van een grootschalige landelijke centraal georganiseerd uitwisselingssysteem van medische gegevens via het (private) EPD-LSP systeem.

Ook toen de rechter in Amsterdam (in een zaak aangespannen door de stichting KDVP) oordeelde dat die zorgverzekeraars werken op grond van een gedragscode die strijdig is met het EVRM.

Ook toen onomstotelijk bewezen werd dat, ondanks alle bezweringen dat men enkel in het EPD-LSP systeem terecht kon komen na daarvoor toestemming te hebben gegeven, de rechter in een uitspraak over de onrechtmatige aanmeldingen moest constateren dat de beheerder van het systeem(VZVZ) niet kon worden verplicht om te garanderen dat zelfs mensen die expliciet bezwaar gemaakt hadden ervan op aan konden dat hun de medische gegevens niet zouden kunnen worden ingezien via het EPD-LSP systeem *door alle professionele zorgverleners en zorgverlenende instanties in Nederland*. Het record van een verklaard tegenstander van het systeem die keer op keer toch weer als zijnde toestemming hebben gegeven bleek aangemeld staat inmiddels op 5x.

> Zie recente berichtgeving hierover van 30 september jongsleden 'Vrijwilligheid LSP een farce bij 4-e en 5e onrechtmatige toestemming ' https://www.zorgictzorgen.nl/vrijwilligheid-lsp-een-farce-bij-4-e-en-5e-onrechtmatige-toestemming/

Ook toen vanuit het veld vanuit de huisartsenpraktijken, tegen alle tegenwerking van het ministerie in, via het 'White box' systeem bewijs geleverd werd dat een veilig en werkzaam alternatief, met behoud van medisch beroepsgeheim en privacy van patiënten, geen onrealistische wensdroom betreft, maar gewoon in de praktijk realiseerbaar is. Zie voor meer info hierover https://whiteboxsystems.nl/actueel.

Pas toen de in arren moede ingestelde Stuurgroep Gespecificeerde Toestemming aan minister Bruno Bruins op VWS eind 2018 rapport uitbracht dat het elektronisch regelen van de gespecificeerde toestemming niet uitvoerbaar was voor burgers, patiënten en zorgaanbieders, omdat het per

individu om het regelen van zo'n 160 vormen van toestemming zou gaan *die ook te allen tijde weer moesten kunnen worden gewijzigd*, zag de minister in dat er pas op de plaats gemaakt diende te worden met het realiseren van een Online-ToestemmingsVoorziening(OTV) voor opvraagbaar gemaakte zorgdata. Lees 'Minister Bruins in mijnenveld verdaagd door standstil rond gespecificeerde toestemming' https://www.zorgictzorgen.nl/minister-bruins-in-mijnenveld-verdaagd-door-gespecificeerde-toestemming/

Helaas moeten wij constateren dat nu minister Bruins is bezweken onder zijn taken, en de momenteel voor de Volksgezondheid verantwoordelijke bewindslieden hun handen vol hebben aan het crisisbeheer van de Corona pandemie, de zorgverzekeraars hiervan gebruik proberen te maken om alsnog hun zin door te drijven met het voorstel van een aan het EPD-LSP gekoppeld Mitz systeem als landelijke online toestemmingsvoorziening(OTV).

Als bijlage 2 voegen we hier het visiedocument 'Overzicht van belangrijkste problemen bij verwerking van bijzondere persoonsgegevens in de gezondheidszorg' dat Vrijbit begin dit jaar heeft aangeboden aan de Autoriteit Persoonsgegevens.

Naast onze principiële bezwaren achten wij het tevens van belang om nog enige kanttekeningen te plaatsen bij het concrete voorstel van Mitz.

Het systeem wat de roepnaam Mitz heeft meegekregen van de, voor dit doel in het leven geroepen, koffiedrinkende stripfiguur met sproeten die met één druk op de knop via haar computer toestemming geeft aan **een private organisatie** om de toegang tot haar medische gegevens te beheren. https://www.programma-otv.nl/ is ongetwijfeld bedoeld als knipoog naar het beginsel 'geen wettelijke grondslag voor het mogen uitwisselen mits daarvoor toestemming is gegeven.

Los van de principiële onwenselijkheid van het optuigen van een grootschalig, landelijk ICT systeem voor het vastleggen en beheren van de invulling van de wijze waarop alle inwoners van Nederland buiten de medische behandelrelatie om, eventueel hun *(ten allen tijde te wijzigen)* toestemming zouden laten vastleggen voor het, voor bepaalde doeleinden en aan bepaalde zorgverleners, ter beschikking stellen van hun medische gegevens, is het in handen willen geven van zo'n systeem aan een private partij onverantwoord.

Toelichting

Mitz als private partij zal in de voorgestelde constructie niet eens juridisch aanspreekbaar te kunnen worden gesteld voor misstanden, vanwege de beoogde opzet van de bedenkers van Mitz om er geen rechtspersoonlijkheid aan toe te kennen. Mitz als derde partij, *die de toegang tot meest gevoelige persoonsgegevens van miljoenen inwoners van Nederland zou gaan beheren*, kan analoog aan de beheerder van het EPD-LSP(VZVZ) haar verantwoordelijkheid ontlopen voor het beheer van het systeem zolang ze de verantwoordelijkheid voor foute registratie of onrechtmatig gebruik bij de gebruikers van het systeem belegd.

Dat met het voorstel voorbij wordt gegaan aan het feit dat men juridisch een wettelijke taakuitvoering niet in handen kan geven aan een systeem is absurd.

Dat daarbij willens en wetens uit het oog wordt verloren dat alleen al om gegevens in het Mitz op te nemen op zich ook vooraf toestemming vereist is, achten wij verwijtbaar.

Uit oogpunt van ongewenste belangenverstrengeling, voor het uitwisselen van elektronische zorgdata is het uiteraard ook ongewenst als het beheer van toestemmingen feitelijk in handen komt van de zorgverzekeringsmaatschappijen- hetgeen alleen al door de wijze van financiering intrinsiek het geval zal zijn.

De opzet van een toestemmingsfunctionaliteit koppelen aan het onveilige en niet functionele EPD-LSP systeem (waarvan alleen al alle principiële randvoorwaarden ten aanzien van toestemmingsvereisten een farce blijken) is een uitermate dom en verwerpelijk idee.

Tot Slot

De conclusie van bovenstaande kan niet anders luiden dan dat het voorstel van de zorgverzekeraars en VZVZ inhoudelijk onacceptabel is.

Waarbij we opmerken dat het ons inziens ook van een totale minachting van de parlementaire democratie getuigt om buiten de aan de Kamer toegezegde parlementaire beraadslaging met de minister om, alsnog te proberen om de wettelijk onaanvaardbare manier van generieke toestemmingsverlening, voor het uitwisselen van medische gegevens, alsnog gewoon in gang te zetten. Net zoals er, zonder dat de betrokkenen daarvan in kennis werden gesteld, of het parlement vooraf werd geïnformeerd, afgelopen voorjaar van iedereen die geen toestemming voor aanmelding in het EPD-LSP had gegeven(tenzij men daar uitdrukkelijk bezwaar tegen had laten vastleggen), gewoonweg werd geregistreerd dat zij toestemming zouden hebben gegeven voor het uitwisselen van hun medische data via dit systeem.

Wij gaan ervan uit dat deze inbreng op de consultatie, net als het geval is bij andere bijdragen, niet wordt voorgelegd aan VWS direct ter beschikking wordt gesteld aan het ministerie van VWS, maar ter reactie zal worden doorgestuurd naar ZN en VZVZ.

Vanwege het groot maatschappelijk belang dat, ook in tijden van de Corona pandemie, het respecteren van de fundamentele burgerrechten en het behoud van het medisch beroepsgeheim niet het loodje leggen, zijn we zo vrij om zowel het ministerie, de parlementsleden als de toezichthouder voor de bescherming van persoonsgegevens te verwittigen over de zoveelste poging van de zorgverzekeraars om inbreuk te maken op de basisprincipes waaraan de wettelijk verankerde toestemmingsvereisten zijn vastgelegd.

Wij verzoeken u om ons een bewijs van ontvangt van deze inbreng te doen toekomen.

Met vriendelijke groet

Namens het bestuur van Burgerrechtenvereniging Vrijbit,

J.M.T.Wijnberg-voorzitter

Bijlage 1

13-2-2014 Data grabbing in de zorg en de privacy van pseudonimisering

http://www.vphuisartsen.nl/uitgelicht/data-grabbing-de-zorg-en-de-privacy-van-pseudonimisering/

Analyse Databanken met persoonsgegevens vormen niet alleen een bedreiging voor de privacy, maar ook een machtsmiddel in het Informatietijdperk. Daar lijken zorgverzekeraars in Nederland zich terdege van bewust, betoogt redacteur Ronald Huissen van het Platform Burgerrechten.

In Groot-Brittannië mogen medische gegevens uit het Britse elektronisch patiëntendossier binnenkort worden doorverkocht aan private partijen die deze data gebruiken om 'de zorg te verbeteren', zo viel vorige maand in The Guardian te lezen. Deze gegevens worden weliswaar gepseudonimiseerd, maar dat vormt geen garantie dat deze informatie niet meer herleidbaar is tot een persoon. Gecombineerd met andere (medische) data is het volgens de beheerder van het Britse EPD 'theoretisch' mogelijk dat bedrijven een specifiek persoon aan de gepseudonimiseerde gegevens kunnen koppelen.

Patiënten hebben weinig vertrouwen

Patiënten hebben zich stevig uitgesproken tegen het plan, wijzend op de gevoeligheid van medische informatie. Het is volgens de patiëntenorganisatie medConfidential een grote vrees van patiënten dat hun gegevens voor commerciële doeleinden gebruikt worden en uiteindelijk onder ogen komen van partijen als werkgevers en verzekeraars. De patiënt heeft namelijk geen zicht op wat er met zijn gegevens gebeurt nadat deze bij het EPD 'de deur uit' zijn. Er is daarbij weinig vertrouwen in het pseudonimiseren van deze gegevens: 'Rather than prevent this, the care.data scheme is deliberately designed so that 'pseudonymised' data – information that can be re-identified by anyone who already holds information about you – can be passed on to 'customers' of the information centre, with no independent scrutiny and without even notifying patients. It's a disaster just waiting to happen.' The Guardian

De Nederlandse situatie

Met de ontwikkelingen omtrent de invoering van een elektronisch patiëntendossier in ons land – een door de Eerste Kamer weggestemd EPD dat in private vorm (LSP) doorstart kreeg, maar tot op de dag van vandaag veel privacyzorgen baart – roept het nieuws uit Groot-Brittannië de vraag op hoe realistisch dit scenario in Nederland is.

Het Nederlandse LSP is vooralsnog niet toegankelijk voor zorgverzekeraars. Volgens de huidige wetgeving zijn in principe uitsluitend zorgverleners die bij een behandeling betrokken zijn, gerechtigd om het medisch dossier van een patiënt bij een andere zorgverlener in te zien via het LSP. Voor iedere persoon of organisatie die niet is aangemerkt als zorgverlener, is het EPD verboden terrein.

UZI-pas

Het Nederlandse LSP is daarmee “slechts” toegankelijk voor een paar honderdduizend zorgverleners met een zogeheten UZI-pas. Organisaties en personen die niet kunnen beschikken over een UZI-pas kunnen in Nederland via het LSP geen medische informatie opvragen.

Het EPD is echter niet het enige landelijke informatiesysteem met medische gegevens van Nederlandse burgers. Er bestaat sinds tien jaar een andere grote databank met medische gegevens, waaruit net als bij het Britse EPD gepseudonimiseerde medische gegevens worden verstrekt aan tal van organisaties en instellingen. Ook hierbij is sprake van flinke privacybezwaren met betrekking tot de herleidbaarheid van deze gegevens.

Het andere EPD

Zorgverleners in Nederland zijn verplicht om op de declaratiefactuur aan de zorgverzekeraar een variëteit aan behandelinformatie aan te leveren. Deze informatie gaat tegelijkertijd in gepseudonimiseerde vorm naar een landelijke database, het zogeheten DBC-Informatiesysteem (DIS), opgericht in 2004. Het DIS bevat daarmee informatie over alle bij verzekeringen gedeclareerde zorgbehandelingen in Nederland.

Het DIS bevat daarmee ook informatie over het bestaan van gezinsproblemen, drank en drugsgebruik, financiële problemen en problemen met politie en justitie.

Om wat voor informatie gaat het concreet? Allereerst moet de zogeheten DBC (Diagnose Behandel Combinatie), een administratieve code die een diagnose en de bijbehorende behandeling weergeeft, worden aangeleverd. Bij behandelingen in de geestelijke gezondheidszorg wordt bij het DIS ook informatie aangeleverd over psychosociale en omgevingsfactoren, voorzien van een waardering die de ernst van deze factoren weergeeft. Het DIS bevat daarmee ook informatie over het bestaan van gezinsproblemen, drank en drugsgebruik, financiële problemen en problemen met politie en justitie. Deze informatie moet sinds 1 januari 2014 ook worden verwerkt in de zorgvraagzwaarte informatie die zorgverleners verplicht moeten gaan aanleveren bij zorgverzekeraars.

Het DIS wordt beheerd door een organisatie genaamd DBC-onderhoud. Onlangs is besloten dat het functioneren daarvan geheel valt onder de verantwoordelijkheid van de NZa, de marktmeester van de zorg. Het doel van de gegevensverzameling in het DIS is door middel van statistische analyse meer zicht en daarmee grip krijgen op zorgkosten.

DIS verzorgt data-uitleveringen

‘Door DIS wordt het medisch handelen en de bekostiging daarvan transparanter. Daarnaast is DIS van belang voor het monitoren van marktontwikkelingen en de ontwikkeling en het onderhoud van het DBC-systeem’, zo valt te lezen op de website van het DIS. ‘DIS zorgt voor een veilig beheer en verzorgt wettelijke data-uitleveringen aan een vijftal publieke afnemers. Na toestemming van de data-eigenaren kan DIS ook informatie leveren aan derden, bijvoorbeeld voor beleids- of wetenschappelijk onderzoek.’

Minister Edith Schippers van Volksgezondheid beantwoordde in mei 2012 Kamervragen van SP-Kamerlid Renske Leijten, die de minister vroeg hoeveel personen toegang hebben tot het DIS, en hoeveel daarvan niet gebonden zijn aan het medisch beroepsgeheim. De minister antwoordde daarop:

Maar over de vraag of de medische gegevens in het DIS daadwerkelijk niet te herleiden zijn naar een persoon bestaan gegronde twijfels.

DIS-gegevens zijn gepseudonimiseerd, het is daarom niet mogelijk tot personen te herleiden gegevens uit het DIS te herleiden. Het medisch beroepsgeheim en medisch tuchtrecht zijn dan ook niet van toepassing op deze gegevens. Over het exacte aantal mensen dat van de verschillende betrokken partijen toegang heeft tot deze gegevens heb ik geen gegevens.

Maar over de vraag of de medische gegevens in het DIS daadwerkelijk niet te herleiden zijn naar een persoon (en daarmee juridisch niet als persoonsgegevens gelden) bestaan gegronde twijfels. Evenals in Groot-Brittannië kan de gepseudonimiseerde informatie in het DIS door koppeling aan informatie in andere bestanden in theorie vrij eenvoudig worden herleid tot personen. Dit is mogelijk wanneer deze informatie gekoppeld wordt aan gegevens die elders al bekend zijn over een persoon. Dat stelt Platformdeelnemer KDVP op basis van een uitvoerige analyse van de wijze van de pseudonimisering in het DIS[1].

Herleiding door middel van ontoereikende pseudonimisering

Dit komt door de wijze waarop de gegevens in het DIS zijn versleuteld; de pseudonimisering bestaat uit de versleuteling van de naam, geboortedatum, postcode, geslacht en Burgerservicenummer van de in het DIS opgeslagen behandelinformatie. De informatie over diagnose, behandeling, medicatie, psychosociale factoren en omgevingsfactoren wordt echter niet versleuteld, evenmin als de begin- en einddatum van behandelingen, de behandelaar in kwestie en de verzekeraar waarbij de behandelkosten zijn gedeclareerd.

De naam van de persoon staat niet bij de behandelinformatie, maar alle bij één persoon uitgevoerde behandelingen staan wel aan elkaar gekoppeld.

Daarbij eist de systematiek van het DIS dat verschillende behandelingen moeten kunnen worden gekoppeld aan één persoon. Met andere woorden, de naam van de persoon staat niet bij de behandelinformatie, maar alle bij één persoon uitgevoerde behandelingen staan wel aan elkaar gekoppeld.

Zo is het in de praktijk zeer wel mogelijk om op basis van bijvoorbeeld de begin- en einddatum van een behandeling, de betreffende verzekeraar en de diagnose- en behandelinformatie in DBC's, een match te maken met informatie die op dat moment al aanwezig is bij zorgverzekeraars of andere organisaties die beschikken over gegevens in de gepseudonimiseerde persoonsdossiers van het DIS. Op die wijze valt deze informatie, indirect, te koppelen aan individuele personen. In het verlengde van deze herleidingsmogelijkheden zou het zelfs mogelijk zijn om de encryptieformule te kraken.

Persoonsgegevens als grootkapitaal in het Informatietijdperk

Het op grote schaal opslaan van medische persoonsgegevens bij zorgverzekeraars en in de landelijke database DIS leidt al sinds de invoering van het DBC-systeem tot veel weerstand onder zorgverleners. Niet alleen vormt de verplichte aanlevering van medische gegevens door zorgverleners een structurele inbreuk op het beroepsgeheim en de privacy van patiënten, ook trekken zorgverzekeraars steeds meer sturingsmacht naar zich toe nu ze over steeds meer informatie kunnen beschikken.

Dat laatste benadrukt Ab van Eldijk, voorzitter van Platformdeelnemer Stichting KDVP in een analyse die onlangs op deze site verscheen. Van Eldijk wijst op een fenomeen dat hij *resource grabbing*

noemt; het op grote schaal vergaren en in bezit nemen van nieuwe, nog niet toegeëigende hulpbronnen. Het is een proces dat leidt tot een fundamentele herverdeling van de economische en bestuurlijke macht.

Partijen die in de eerste fase van deze ontwikkeling toegang weten te krijgen tot cruciale informatie, weten zowel financieel-economische als (semi-) publieke sturingsmacht op te bouwen.

In de 16e eeuw vond een dergelijke ontwikkeling plaats in de Britse landbouw. Toen landbouwgronden interessant bleken voor commerciële producties, werden gemeenschappelijke gronden afgebakend en tot individueel bezit gemaakt, wat leidde tot veel verzet onder boeren. Deze ontwikkeling veroorzaakte een fundamentele wijziging van de machtsverhoudingen in de samenleving.

In de huidige informatiemaatschappij, waarvan we op dit moment de beginfase meemaken, is *Big Data* die nieuwe hulpbron. Met de ontwikkeling van informatietechnologie is het mogelijk geworden om op grote schaal informatie te verzamelen, op te slaan en selectief uit te lezen. Partijen die in de ongereguleerde eerste fase van deze ontwikkeling op grote schaal toegang weten te krijgen tot cruciale informatie, weten snel zowel financieel-economische als (semi-)publieke sturingsmacht op te bouwen.

Data grabbing

In plaats van het toe-eigenen van landbouwgronden, richten partijen zich anno 2014 op data, het goud van het informatietijdperk. Van Eldijk noemt het *data grabbing*, het verzamelen van zoveel mogelijk data, in het bijzonder persoonsgegevens. Zowel de (semi-)overheid als zorgverzekeraars in Nederland hebben in de afgelopen jaren enorme hoeveelheden medische gegevens kunnen verzamelen door zorgverleners te verplichten tot de aanlevering van diagnose-informatie en behandelgegevens, gekoppeld aan psychosociale en omgevingsinformatie.

Het is een ontwikkeling die stichting KDVP middels beroepsprocedures probeert tegen te gaan. In de rechtszaak die de stichting in 2012 voerde tegen de NZa, gaat Van Eldijk in zijn pleitnotitie [pdf] in op de grote hoeveelheid macht die zorgverzekeraars via hun contracteerbeleid uitoefenen op de zorgverleners wiens behandelingen ze vergoeden, en de hoeveelheid medische persoonsgegevens die zorgverzekeraars daarbij kunnen opeisen.

Gedetailleerde diagnose-informatie

Het contracteerbeleid stelt zorgverzekeraars in de positie om het aanleveren van gedetailleerde diagnose-informatie als harde voorwaarde te stellen aan zorgverleners. Doen zorgverleners dat niet, dan wordt er geen contract afgesloten en hebben zorgverzekeraars de mogelijkheid om zorgverleners extra te korten op vergoeding van de geleverde zorg.

Deze verplaatsing van publieke sturingsmacht naar het contracteerbeleid van zorgverzekeraars wordt gesteund door de minister van Volksgezondheid. Zij heeft het onlangs mogelijk gemaakt dat zorgverzekeraars tot 100 procent korten op een vergoeding van niet gecontracteerde zorg die wordt verleend op basis van restitutie. Met dit beleid steunt de minister het selectieve contracteerbeleid van zorgverzekeraars dat verplicht tot steeds gedetailleerdere digitale informatie-uitwisseling.

Noch de minister noch beroeps- en patiëntenorganisaties leggen zorgverzekeraars daarbij iets in de weg, stelt Van Eldijk: ‘Met groot gemak wordt de controle over uitwisseling en gebruik van medische

persoonsgegevens ingeleverd in onderhandelingen over kostenbeheersing, tarieven, kwaliteit en hoofdbehandelaarschap.'

Centrale sturingsmacht bij zorgverzekeraars

Hiermee is de centrale sturingsmacht in de zorg komen te liggen bij zorgverzekeraars, die zijn uitgegroeid tot de dominante partij in de zorgsector ten koste van de publieke sturing van de zorg en de positie van patiënten en zorgprofessionals.

Beroepsorganisaties en overheid zouden zich moeten realiseren dat door zorgverzekeraars zoveel informatie te laten toe-eigenen, de machtsbalans wezenlijk verschuift. 'Zodra zorgverzekeraars de beschikking hebben over alle informatie, wordt het voor hen mogelijk om als dominante partij in de zorg exclusieve sturingsmacht uit te oefenen', waarschuwt Van Eldijk.

Bijlage 2

Overzicht van belangrijkste problemen bij verwerking van bijzondere persoonsgegevens in de gezondheidszorg.

Binnen de gezondheidszorg spelen in grote lijnen dezelfde issues als genoemd in DEEL I *(helicopterview dataverwerking bij de overheid).*
De wijze waarop uitwisseling, koppeling, analyse en gebruik van persoonsgegevens (verkregen voor uiteenlopende taken en doelen binnen onderscheiden beleidsdomeinen) tussen en door gezondheidsinstellingen en overheidsdiensten nu plaatsvindt maakt dat deze processen niet afdoende kunnen worden gecontroleerd en verantwoord (dit is ook de conclusie van WRR en RvS).

Daarbij vereisen binnen de sector zorg een aantal zaken op dit moment extra aandacht:

- Allereerst is er de problematiek van "gespecificeerde toestemming" bij uitwisseling van medische persoonsgegevens. Waar het uitwisselen en/of delen van medische persoonsgegevens plaats vindt op basis van toestemming moet sprake zijn van specifieke, geïnformeerde toestemming van de betrokkene. Het verlenen van toestemming voor datauitwisseling via enig informatiesysteem voor een niet specifieke, niet welbepaalde doelstelling is inmiddels ook door de politiek aangemerkt als een onjuiste werkwijze die moet worden aangepast.
"Gespecificeerde toestemming" zoals die door een studiegroep is voorgesteld is echter onwerkzaam en onuitvoerbaar gebleken. Halfslachtige oplossingen die nu worden voorgesteld zijn niet rechtmatig, voor patiënten ondoorzichtig (uninformed consent en tevens in strijd met vereiste van voorzienbaarheid), en schaden de vertrouwensrelatie tussen arts en patiënt.
- De implementatie van het LSP en uitbreiding van de inzet van het LSP informatiesysteem voor veel bredere toepassing buiten de weekenddienstwaarneming blijkt te leiden tot ondoorzichtige (niet specifieke, niet welbepaalde) toestemming en het gebrek aan afdoende logging ten behoeve van controle en verantwoording van toestemmingsverlening.
- Tegelijkertijd bestaat er een groot risico voor disproportionele toegang tot medische persoonsgegevens (aanvankelijk had in het huidige systeem 1 op de 25 Nederlanders[1] "inzagerecht" in het LSP; in de nieuwe situatie - met aansluiting van de care sector, paramedici en ketenzorg groeit dit aantal exponentieel[2]). Dit probleem wordt nog vergroot door koppeling van twee centrale infrastructuren voor ziekenhuisbeelden aan het LSP[3].
Deze extreem brede, disproportionele toegang tot medische persoonsgegevens is onaanvaardbaar en is mede gelet op het brede aanvalsvlak niet meer effectief te beveiligen.

- Voor uitwisseling van medische persoonsgegevens bestaan alternatieve open standaarden voor "end-to-end" beveiligde communicatie tussen zorgverleners waarin 'opt-out volgens WBGO' in ICT kan worden ingebouwd en waarmee door rechtstreeks te autoriseren voor specifieke zorgverlening door specifieke bij een behandeling betrokken zorgverleners uit kan worden gegaan van veronderstelde toestemming binnen de regels van medebehandelaarschap. Dit model is inmiddels ook door zorgverzekeraars[4] en VWS[5] aangemerkt als een goede/legitieme (itt huidige werkwijze) en na te streven optie.

- Het verzamelen en verwerken van behandelgegevens voor kwaliteitsmetingen waarvoor deze niet geëigend zijn (zie Rapport Algemene Rekenkamer over kwaliteitsmeting in GGZ) is per definitie *niet noodzakelijk* en dient bijgevolg niet plaats te vinden.

- In het kader van populatieanalyses, kwaliteitsanalyses en de zorgregiovorming worden vaak zonder doelbinding bijzondere medische persoonsgegevens verzameld op centrale locaties zonder dat *een legitieme verantwoordelijke* is aan te wijzen voor verzameling en gebruik van deze bijzondere persoonsgegevens.

- Het verstrekken van medische data aan een centrale locatie is in veel gevallen *niet noodzakelijk* omdat de gezochte analyses door de oorspronkelijke verantwoordelijke partij die over de data beschikt zonder uitwisseling van persoonsgegevens had kunnen worden uitgevoerd binnen het bestand van de oorspronkelijke verantwoordelijke (zie ook problematische werkwijze DIS).

- De wijze waarop medische gegevens op individueel niveau verkregen door zorgverzekeraars en verzameld bij Vektis met doorbreking van doelbinding worden ingezet en gebruikt voor het starten van een datawarehouse gericht op (commerciële) dienstverlening, die werkwijze is niet legitiem en dient gestaakt te worden. In de nu door Vektis verleende diensten kan middels andere minder inbreukmakende, legitieme procedures voorzien worden.

- Daar waar detailcontroles worden uitgevoerd, door zorgverzekeraars of in de Jeugdzorg, ontbreekt het aan de noodzakelijke procedures om te voorkomen dat medische persoonsgegevens die bij detailcontroles verkregen worden alleen onder geheimhoudingsrestricties mogen worden gebruikt in het betreffende controle onderzoek en aansluitend dienen te worden vernietigd. Procedures voor detailcontroles dienen hiertoe te worden aangepast.

- De breed opgezette dataverzameling zoals die op dit moment in de jeugdzorg wordt gestart om kinderen (en personen in hun sociale omgeving) te profileren op risico's is onaanvaardbaar. Het is ook onjuist en onverantwoord dat bij deze dataverzameling ook gebruik wordt gemaakt van CBS-microdata.

B. Toelichtende informatie bij voorgaand overzicht van belangrijkste problemen bij verwerking van bijzondere persoonsgegevens in de gezondheidszorg

Zorg ICT en het belang van vertrouwelijkheid

In de relatie van patiënt met zorgverlener staat vertrouwen centraal bij het beslissen over de meest geëigende behandeling voor de gezondheid van de patiënt. Vertrouwelijkheid is het belangrijkste fundament van de zorgrelatie. Zorgvuldige omgang met medische persoonsgegevens zoals die beschikbaar komen bij de zorgverlening is dan ook expliciet opgenomen in de WBGO en de AVG. Het belang is tweeledig: [6] er is *enerzijds* het gerechtvaardigd privacybelang van de patiënt om in vertrouwen zijn of haar intiemste kennis te kunnen delen om zo de meest afdoende behandeling te kunnen krijgen, en *anderzijds* is er het maatschappelijk belang voor een goed functionerend gezondheidssysteem waarin iedereen zich vrijelijk en zonder vrees bij een zorgverlener moet kunnen wenden zonder dat dit ter kennis komt van anderen dan de hulpverlener. Hierdoor kan worden voorkomen dat een patiënt zich, door twijfel hierover niet - of te laat - meldt.
De vertrouwensrelatie tussen arts en patiënt is zo cruciaal voor goede zorg en de verantwoordelijkheid van de arts voor bescherming van informatie die in deze relatie is verkregen moet dan ook centraal staan in het ontwerp van de ICT-systemen die de opslag, verwerking en gebruik van deze informatie mogelijk maken.

Het concept " *Privacy en security by Design"* moet hierbij centraal staan. Privacy by design is geen statisch eenmalig ontwerp maar een dynamisch proces, waarbij voortdurend de laatste technische inzichten moeten worden uitgewerkt en toegepast[7]. Als er gegevens gedeeld worden moet dit waar mogelijk (voor beschikbaar stellen informatie relevant voor behandeling in noodsituaties zijn al specifieke oplossingen ontwikkeld en beschikbaar) gebeuren met instemming van de betrokkene, de behandeling dienen, en voor de uitvoering van de behandeling (ook in brede zin binnen het huidige gezondheidszorgsysteem) noodzakelijk zijn.

Dilemma's in het ICT-landschap

De ZorgICT kent een aantal zeer moeizame dossiers. Naast het LSP, waarover het laatste woord zeker nog niet gezegd is (knooppunt-ontwerp[8], end-to-end encryptie[9], inhoudelijke technische problemen[10] en kosten[11]) zijn de belangrijkste twee dossiers: 1) Gespecificeerde toestemming (GST) voor berichtenverkeer en het delen van dossierkennis tussen zorgverleners, en 2) de voortdurende vraag om data te delen voor allerhande managementvragen, voor beleid- en voor onderzoek.
Door het vasthouden door politiek, beleidsmakers en managers in de zorg aan oude technieken en ontwikkelingen blijkt het moeilijk, zo-niet onmogelijk, om een ICT-systeem op te zetten waarin *controleerbaar en te verantwoorden* wordt omgegaan met medische persoonsgegevens, terwijl alternatieven inmiddels wel beschikbaar zijn.

GST en berichten delen

Het uitwisselen van berichten vormt de kern van alle primaire processen in de zorg, en het wordt belangrijker met de groeiende samenwerking in ketens en netwerken van zorgverleners die gezamenlijk de zorg aan patiënten leveren. Het zonder problemen kunnen delen van dossierkennis tussen zorgverleners staat daarom ook bovenaan het wensenlijstje van zorgverleners, patiëntengroepen en politiek. Het inmiddels oude issue hierbij is "het regelen van toestemming":
"Nu … blijkt dat voor de gegevensverwerking door VZ[V]Z geen beroep mogelijk is op artikel 21 eerste lid onder a Wbp en ook niet op artikel 7:457 tweede lid BW, blijft voor de gegevensverwerking door VZ[V]Z, vanwege het wegvallen van uitzicht op een specifieke wettelijke regeling, uitsluitend een beroep over op 'uitdrukkelijke toestemming'."[12]

Via de wet Cliëntrecht voor de Zorg is eerst getracht te regelen hoe toestemming moet gaan plaats vinden. Hierbij geeft de patiënt aan dat hij toestemming geeft medische gegevens door te geven voor een specifiek doel en een specifieke zorgverlener. Voor het doorgeven van gegevens aan een nieuwe (categorie) zorgverlener(s) moet wederom toestemming worden gevraagd. We zien hier dat in feite de "specifieke toestemming" die idealiter in een goed doordacht systeem moet worden ingebouwd al wordt verdund tot – wat de toenmalige Minister strategisch voorstelde als – "gespecificeerde" toestemming.

Een werkgroep van experts zocht uit hoe een dergelijk systeem vorm moet krijgen (project Gespecificeerde Toestemming – GST), maar kwam in de zomer van 2018 tot de conclusie dat minimaal 160 categorieën te onderscheiden zijn, met evenzovele vinkjes die door een patiënt zouden moeten worden gezet[13]. Een onwerkbare situatie voor zorgverleners (die de toestemming moeten vragen en vastleggen), voor patiënten (die door de bomen het bos niet meer zien) en voor ICT-leveranciers (die zeer complexe toestemmingen moeten programmeren).

De huidige Minister heeft voorgesteld dat een minder complex systeem wellicht een oplossing kan bieden[14], waarbij echter voorbijgegaan wordt aan het fundamentele probleem ten aanzien van het concept van 'gespecificeerde toestemming'. Immers, de AVG schrijft voor dat duidelijk specifiek toestemming moet worden gegeven voor welk specifiek doel data wordt overgedragen. Terecht werpt de Privacy Barometer op: "*In plaats van medische gegevens nooit te delen* ***tenzij er***

***toestemming is**, worden gegevens in het LSP **altijd gedeeld tenzij dat voor bepaalde categorieën geblokkeerd is**. Deze omgekeerde structuur is een niet te verhelpen basale ontwerpfout.*

Gespecificeerde toestemming is een wettelijk lapmiddel om deze tekortkomingen van het LSP op te vangen…"[15]. Zorgvuldige toestemmingsregels vereisen een wezenlijk ander ontwerp.
Zelfs NICTIZ, de oorspronkelijke hoeder van het LSP, gaf al eerder aan dat de toepassing van nieuwe concepten en een andere opzet deze problemen kunnen voorkomen: een decentrale structuur, waarbij de zorgverlener via push-autorisaties *gericht* en *rechtstreeks* toestemming geeft aan het doelsysteem van de tweede zorgverlener, komt wel tegemoet aan de bezwaren die kleven aan de pull-opzet van veel huidige systemen[16].

Van de door de wet voorgeschreven "gespecificeerde toestemming" is gebleken dat het niet te implementeren is. Het hele probleem van gespecificeerde toestemming kan echter in een decentrale opzet ondervangen worden.

Decentrale infrastructuur standaarden voor implementatie van "opt-out"

Recente ontwikkelingen op het gebied van technologische innovatie bieden een oplossing: de opzet van een open-standaard voor uitwisseling van gegevens zal in 2020 worden vrijgegeven.
De open standaard is eerder succesvol toegepast in de weekenddienstwaarneming in Amsterdam[17] en kan zorgen voor ICT-oplossingen die werken volgens de logica van opt-out: het gaat om rechtstreekse communicatie tussen zorgverleners, zonder *middle-man*, waarbij het mogelijk is te werken volgens de laatste stand van de techniek volgens *privacy en security by design*.
Hierbij worden "inkijk" toestemmingen (linkjes) actief gepusht van de ene zorgverlener naar de andere zorgverlener. Deze linkjes bevatten toestemmingen voor "wat, wie, waarvoor en hoe lang", en hebben het voordeel dat gegevens pas worden opgehaald op het moment van zorg, waardoor de gegevens altijd actueel zijn.
Verschillende experts suggereerden oplossingen in deze lijn, samen met Ron Roozendaal, Chief Information Officer van het VWS, in een blog-discussie afgelopen najaar[18]. De implementatie van de open standaard in de Whitebox laat zien dat identificatie, authenticatie, autorisatie, logging en endto-end encryptie op een flexibele manier kunnen worden geïmplementeerd[19].

De WBGO stelt dat mede-behandelaren gegevens mogen (en moeten) delen als dat noodzakelijk is voor de goede zorgverlening, op basis van veronderstelde toestemming. De nieuwe systematiek voldoet hieraan. Alleen historische gegevens kunnen niet met terugwerkende kracht zonder meer worden doorgegeven.

> De oplossing voor historische gegevens is echter ook al in de systematiek ingebakken: hierbij kan gebruik gemaakt worden van de Nederlandse organisatie van het zorgstelsel waarbij de huisarts als centrale zorgverlener fungeert en medebehandelaar is van alle zorg voor de patiënt. De huisarts kan zo van alle specialisten en apothekers ook historische gegevens pvragen/ontvangen. De vernieuwende open standaard maakt het mogelijk dit te doen door in het huisartsensysteem "inkijk" toestemmingen aan te maken voor informatie in dossiers van overige zorgverleners die eerder bij de behandeling van een patiënt betrokken zijn geweest, waardoor de huisarts feitelijk een virtueel dossier opbouwt van alle gegevens van zijn patiënten. De huisarts kan vervolgens ook historische data, dan wel linken naar historische patiëntgegevens aanwezig bij andere zorgverleners, delen met mede-behandelaren.

De open standaard bevestigt hiermee eigenlijk de praktijk in Nederland waarbij de huisarts de spil is in het zorgstelsel, degene die overzicht houdt over alle zorg die aan de inwoners van Nederland wordt geleverd. En met het systeem wordt feitelijk een spinnenweb van linkjes opgebouwd die het zorgpad rond de patiënt volgt. De techniek biedt de huisarts zo bijvoorbeeld - naast security en privacy by designfuncties - inzicht in wat is gedaan met een doorverwezen patiënt en tevens in de interne doorverwijzingen en onderzoeken binnen een ziekenhuis.

Voor de implementatie is het belangrijk dat initiatieven zoals NUTS, waarin ICT-leveranciers gezamenlijk werken aan oplossingen voor decentrale en rechtstreekse communicatie tussen zorgsystemen. NUTS[20] laat zien dat de ICT-sector zelf ook neigt naar een snelle uitrol van deze decentrale oplossing voor de jarenlang slepende kwestie van kwestie van gegevensuitwisseling terwijl niet voldaan werd aan het vereiste van specifieke toestemming. Doorgaan met “reparaties” aan het huidige centrale systeem is trekken aan een kreupel - dan wel dood - LSP paard. Binnen NUTS wordt op dit moment bijvoorbeeld gemeenschappelijke software ontwikkeld die door alle deelnemers van NUTS gebruikt mag worden voor identificatie en authenticatie. Implementatie van de nieuwe open standaard voor berichtenuitwisseling kan worden ingebouwd in de XIS-systemen zelf, het kan als een module aan het XIS worden gehangen binnen het domein van het XIS, of er kan een aparte applicatie buiten de XISsen komen die op een API van het XIS aansluit (voor deze laatste optie is in Amsterdam gekozen door de huisartsen die de Whitebox gebruiken).

Decentrale privacy vriendelijke oplossingen vergen een specifieke benadering in de ontwerpfase om de nodige flexibiliteit in te bouwen die het mogelijk maakt om rekening te houden met lokale contexten[21]. Maar eenmaal ontworpen blijken de oplossingen niet alleen flexibeler, maar ook eenvoudiger in opzet en onderhoud, en daarmee goedkoper.[22] De keuze voor een veilige flexibele (noodzaak gegeven de dynamiek van ontwikkelingen in de zorg) en daarmee toekomstbestendige oplossing is dan niet moeilijk te maken!

Secundaire processen in de zorg: hergebruik van data in andere contexten

In de zorg worden naast processen die direct relevant zijn voor het eigenlijke proces van zorgverlening de primaire processen genoemd, terwijl ondersteunende processen zoals administratie, declaratie, verantwoording, beleid en onderzoek als secundaire[23] (of soms ook tertiaire[24]) processen worden aangemerkt.
Voor sommige processen geldt een wettelijke basis die vereist dat zorgverleners verantwoording afleggen voor geleverde zorg in de vorm van declaraties of het aanleveren van bepaalde informatie voor verantwoordingsdoeleinden.
Hoewel een wettelijke basis, mits voorzien van duidelijke expliciete legitieme doelen, een reden kan vormen voor de verplichting van doorlevering, moet blijvend in het oog worden gehouden of de gegevensdeling nog steeds voldoet aan eisen van subsidiariteit en proportionaliteit gezien de huidige stand van de techniek.
Over de aanpak van verbetering van het gebruik van gegevens in de gezondheidszorg bestaat in Nederland consensus over het feit dat zorgvuldige registratie cruciaal is voor inzet van de data in de primaire processen en het hergebruik van gegevens voor afgeleide zorgprocessen. Het belang van goede registratie komt bijvoorbeeld tot uiting in stimuleringsregelingen voor huisartsen om volgens richtlijnen en standaarden te registreren en leidde in ziekenhuizen tot een standaardiseringsproject “registratie aan de bron”.
Het belang van standaarden is ook groot door de wens voor hergebruik van klinische data en afgeleide gegevens. In Europa wordt daarom ook het idee gestimuleerd dat gegevens vindbaar (metadata), toegankelijk (protocollen rond toegang), te koppelen en herbruikbaar voor meerdere processen (FAIR) moeten zijn.

Het belang van context

De mogelijkheid tot nuttig delen van data valt of staat bij een zorgvuldige registratie en een zorgvuldige interpretatie van de gegevens en of die in een andere context ook inhoudelijk geldig en interpreteerbaar zijn. Dit geldt natuurlijk voor primaire processen, maar evenzeer voor secundaire processen, als verantwoording en onderzoek.
Bij het ontbreken van de mogelijkheid tot het interpreteren van data is de doorlevering zelf verworden tot een nutteloos, gevaarlijk (onjuiste conclusies), niet noodzakelijk en daarmee illegaal- proces[25].

Bij processen van autorisatie door brongebruikers voor gebruik van informatie door derden in secundaire processen is het dus niet alleen consideratie voor het recht op bescherming van de persoonlijke levenssfeer, of zinvol gebruik van data buiten de context, maar moet dus rekening worden gehouden met de bruikbaarheid/onbruikbaarheid van brongegevens in een volgende context van zorg of onderzoek.

Feitelijk bevat dus de toestemming ook altijd impliciet een volgend doel en de onderliggende aannames over het nut en de mogelijk onjuiste interpretatie van gegevens in de volgende context.
Autorisatie als zorgvuldig proces is noodzakelijk voor het behoud van de vertrouwelijkheid van de behandelrelatie, waarbij de patiënt erop moet kunnen vertrouwen dat alleen informatie gedeeld zal worden als dit noodzakelijk en zinvol is. Van belang is op te merken dat de wetgever het doorleveren van medische persoonsgegevens afwijst *behoudens* uitzonderingsgevallen, waarbij *gerichte* gegevensdeling alleen gewenst is voor de goede behandeling bij mede-behandelaarschap, in uitzondering bij levensbedreigende situaties voor de patiënt, of onder stikte voorwaarden en waarborgen voor *zinvol* wetenschappelijk en/of statistisch onderzoek voor *het algemeen belang*.

'Hergebruik' van data verwordt tot oneigenlijke dataverzamelwoede buiten het zorgproces

Al bij aanvang van het DBC-Informatie Systeem (DIS) uitte het toenmalige College Bescherming Persoonsgegevens haar zorgen over deze "meest risicovolle gegevensverwerking" van Nederland.
Dit systeem bevat alle DBCs uit de GGZ en de tweedelijns zorg, en was opgezet om de secundaire processen van onderhoud van het zorgstelsel (opstellen van "zorgproducten", risicoverevening en beleid) te ondersteunen. Al vroeg in 2009 werd geconcludeerd dat het systeem feitelijk overbodig was, niet alleen op gronden van herleidbaarheid en risico's voor de privacy, maar vooral ook vanwege argumenten van subsidiariteit en proportionaliteit: die doelen kunnen op een andere manier bereikt worden (de Vos, 2010).
Het DIS staat niet alleen; Vektis, verschillende - al dan niet academische onderzoeksinstituten, SBG een meer recent Regionale Samenwerkingsverbanden (RSOs), vertonen hetzelfde euvel. Er moet in de ogen van deze partijen veel data verzameld worden omdat het inzicht kan verschaffen voor beleid, en omdat er zulk mooi onderzoek mee zou kunnen worden gedaan.

Het is geen uitzondering dat huisartsenpraktijken meer dan 12 keer per jaar een volledige kopie van hun brondatabase laten maken voor "ondersteuning" en "onderzoek" door verschillende ICT-leveranciers, onderzoekspartijen of innovatieve projecten. De meeste huisartsen hebben echter geen idee wat er met de data gebeurt en overzien de gevolgen niet van de proliferatie van medische (onderzoeks) databestanden in Nederland.
Verschillende klachten over de privacy en het oneigenlijk grootschalig gebruik van data liepen uit op grote bijstellingen en onderzoek naar oneigenlijk gebruik en voortslepende rechtszaken.
Gebruik van brondata voor secundaire processen is echter aan regels gebonden en vereist een zorgvuldige analyse van doelen, nut en mogelijke alternatieven die het mogelijk maken voor zorgverleners om controleerbaar en te verantwoorden data te delen.

Brondata voor beleid en onderzoek: controleerbaar en te verantwoorden

Een afweging voor de manier waarop medische persoonsgegevens als brondata kan worden hergebruikt in secundaire processen kan pas gemaakt worden door per proces te kijken naar aspecten van noodzaak, doelbinding, proportionaliteit en subsidiariteit. Begrip van de stand van de techniek is nodig om het laatste aspect goed te evalueren.
De zorg in Nederland kent verschillende secundaire processen waarin brondata een bijdrage kan leveren aan het goede verloop van de voorhanden taken. We kunnen de volgende processen onderscheiden:

- Declaraties en aanverwante logistieke informatie (bv. start/stop berichten en wachtlijsten)
- Interne kwaliteitsrapportages en zorgprocesrapportages voor monitoring en intern beleid
- Externe kwaliteitsrapportages en indicatoren

- Monitoring van infectieziekten en preventieve gezondheidszorgmonitoring (bv. borst- en darmkanker)
- Wetenschappelijk onderzoek
- Statistiek en regionaal en landelijk beleid
- Rapportages of gegevensoverdracht voor fraudeonderzoek

Naast de voorwaarden die aan de bewerkingen worden gesteld (nooit doorleveren *mits*) eist de AVG bij de bewerking van medische persoonsgegevens dat ICT-ondersteuning wordt opgezet volgens de principes van privacy by design.

Privacy by Design

Op dit moment worden voor veel van deze processen grote hoeveelheden data doorgezonden. Dit kan beter. Bij een zorgvuldige ICT-ondersteuning van deze processen kunnen de volgende tactieken van Privacy by Design[26] in ogenschouw worden genomen:
- Dataminimalisatie (zorg dat nooit meer brondata dan nodig wordt gebruikt en dat deze alleen zo lang als nodig kan worden gebruikt; gebruik bijvoorbeeld ja/nee berichten i.p.v. van het tonen van een identiteitsbewijs of digitale persoonsgegevens[27])
- Scheiden van data (Feitelijk is het isoleren van brondata een vorm van scheiding. Waar mogelijk zouden XISsen dit ook moeten toepassen op de databases van zorgverleners, die nu vaker wel dan niet worden opgeslagen in 1 grote zorgdatabase, zonder muren tussen verschillende praktijken, ziekenhuizen, of specialisten in ziekenhuizen)
- Abstraheren (Hier kan worden gedacht aan aggregatie van data in groepen of geografische gebieden met samenvattende tellers en noemers, het uitsmeren of verstoor gegevens, zoals bijvoorbeeld in de WoonZorgwijzer wordt toegepast met weergaves van patronen van dichtheden, zonder dat exacte locaties of aantallen kunnen worden bepaald).
- Verbergen (zorg dat er geen toegang is, encrypt, ontkoppel (!) of anonimiseer.

Daarnaast vereist werken volgens Privacy by Design dat de databewerking controleerbaar en te verantwoorden is en dat betrokkenen (zowel zorgverleners als patiënten) geïnformeerd zijn over de bewerkingen en deze begrijpen.

Naar een systeem van verantwoorde secundaire proces-ondersteuning

Als we dataminimalisatie serieus nemen wordt het snel duidelijk dat vrijwel alle secundaire processen afgedaan kunnen worden met geaggregeerde data. Voor zowel declaraties, kwaliteitsrapportages, beleid, statistiek en ook een groot deel van het onderzoek kan voldaan worden met geaggregeerde data.

Hoe kan een PbD-systeem voor secundaire processen eruit zien? Al in 2010 stelde Hugo de Vos dat het genereren van indicatoren in bronsystemen voor de GGZ de voornaamste kwaliteitsindicatoren kunnen opleveren voor beleid en onderzoek. Een dergelijk systeem kan worden ondersteund door een ICT-voorziening waarin centraal indicatoren definities kunnen worden aangemaakt die via bevraging in bronsystemen.
De enige centrale opslag die nodig blijft is de opslag van tellers en noemers in een benchmark per zorgverlener/patiëntengroep. Uiteraard dient het systeem zo te worden opgezet dat de aggregatie niet zodanig is dat toch personen kunnen worden herkend, dat alleen de bevoegde organisatie(s) vragen kunnen stellen, dat er controle is op elke analyse die wordt aangemaakt en op het delen van indicatoren met derde partijen (een zorgverlener kan dan zelf bepalen met welke (groep) andere zorgverleners hij wil benchmarken). Een dergelijk systeem is in ontwerp beschreven in een pilotstudie van het UMCU voor de GGZ-sector[28] en verder uitgewerkt in opdracht van een aantal ICTleveranciers[29].

Aansluitend op deze initiatieven wordt op dit moment ook geëxperimenteerd met het beschikbaar maken van een stapelmonitor voor zorg, wonen en welzijn in het kader van ZonMW projecten voor de Juiste Zorg op de Juiste Plek. Hierin wordt een regionale portal opgezet met een stapelmonitor voor gemeentelijke of regionale samenwerkingsverbanden waarin op geaggregeerd niveau patronen

en trends kunnen worden ontdekt over zorg in breder verband. 1 op 1 koppeling van persoonsgegevens blijkt onnodig.
Alleen wanneer het om intern beleid, evaluatie en leerprocessen in het zorgproces zelf gaat is het vaak wenselijk ook patiëntgegevens te *kunnen* zien, maar omdat dit onderdeel is van het interne zorgproces is dit een legitieme bewerking.
Voor externe kwaliteitsindicatoren, beleid, of zelfs monitoring van infectieziekten of registraties van bepaalde ziektes is een dergelijke systematiek waarmee op geaggregeerd niveau patronen en trends kunnen worden ontdekt voldoende.

Hoe kan de zorgverzekeraar in een dergelijke systematiek nog haar formele en materiële controle uitvoeren? Mogelijk kan ICT hier een verlichtende rol in spelen; zorgverlener zendt verzekeringsnemer id naar Vecozo → Vecozo controleert het recht op en omvang van (type) behandeling → zorgverlener krijgt antwoord en kan al dan niet behandeling aanpassen aan het verzekerde pakket. Bij het voorstellen van een behandeltraject kan een dergelijke werkwijze worden gehanteerd: zorgverlener doet voorstel behandeling → de DBC-router controleert of behandeling en diagnose overeenkomen → bij een geldige combinatie mag behandeling worden uitgevoerd en gedeclareerd.

Eerder wees het College Bescherming Persoonsgegevens al op een dergelijke systematiek.
Het CBP wijst in dit kader ook op betere 'controle aan de poort', wat inhoudt dat de zorgverleners zelf controles uitvoeren bij het in behandeling nemen van een patiënt. Dit kan bijvoorbeeld een controle zijn van de verzekeringsaanspraken. Zo zal de noodzaak van een deel van de controle door de zorgverzekeraar - en de bijbehorende informatiestroom - wegvallen[30].
Met een dergelijke systematiek kan in principe een groot deel van de gegevensstroom met medische data wegvallen. Wel dient de verzekeringsmaatschappij controlemogelijkheden te behouden om te kunnen inschatten of er geen ongeoorloofde dingen gebeuren. Dit kan – en zal in praktijk door verzekeringen zelf ook – meestal door indicatoren en samenvattende rapporten kunnen worden afgedekt.

Voor het systeem van start-stop berichten alsmede andere controles aan de poort bij gemeentelijke zorgtrajecten is het zeer wenselijk dat de nieuwste technieken worden toegepast zoals het IRMA[31] identificatie systeem of Trusttester van TNO, waarbij door middel van attributen getest kan worden of iemand recht heeft op zorg, een uitkering, toeslagen o.i.d., zonder dat hele bestanden gedeeld hoeven te worden of te worden verzameld in steeds op nieuw te actualiseren hulpbestanden waarin recht op bepaalde hulp wordt gecontroleerd[32].
Alleen voor *zinvol* wetenschappelijk onderzoek in het *algemeen belang* door betrouwbare partijen kan het ook wenselijk zijn data te kunnen koppelen. Hier kunnen technieken van toegang, toestemming en logging wel een rol spelen bij het ICT-technisch implementeren van governance afspraken, zoals op dit moment wordt verkend in het Person2data project van de UvA, Amsterdam[33].
Mogelijk kan verder de "Personal Health Train"-techniek in de toekomst een vervanging worden van het kopiëren van data[34].

Gelukkig zijn inmiddels inzichten en ICT-kennis beschikbaar om de steven te wenden en een noodzakelijke, nieuwe, veilige koers te kiezen door het roer om te zetten.

1 Jacobs (2012) The electronic patient record from the perspective of data protection. In: Munichs, Schuijff & Besters; Databases: the promise of ICT, the hunger for information, and digital autonomy. Rathenau Instituut.

2 VZVZ (2015) Businessplan 2016-2020.

3 https://www.zorgictzorgen.nl/onbeschaamde-stimulering-lsp-functionaliteit-met-overheidsgeld-in-twinproject

4 Zorgverzekeraars Nederland: Onderzoek Whitebox; eindrapport 28 oktober 2019, door “We Do Trust” the technology governance company. Rapport in opdracht van Zorgverzekeraars Nederland.

5 “…maak het mogelijk om in de behandelrelatie voor een specifieke vraag digitaal informatie op te vragen met digitaal bewijs van zowel identiteit van de arts als van toestemming van de patiënt. Dat volgt de WGBO en lijkt op de oplossing die Whitebox gebruikt.” Ron Roozendaal, Chief Information Officer VWS, 1 december 2019, https://www.ronroozendaal.nl/blog/2019/12/toestemming-een-bijdrage-aan-de-hoedanwel

6 Nouwt (2012) https://www.zorgkaartnederland.nl/blog/het-medisch-beroepsgeheim-waaromvertrouwelijkheid-belangrijk-is

7 Hoepman (2020) https://www.cs.ru.nl/~jhh/publications/pds-boekje.pdf

8 Een fundamenteel ontwerp-bezwaar tegen centrale infrastructuur is dat een inbraak, hoe goed beveiligd dan ook, kan leiden tot “besmetting” van het hele systeem, terwijl bij netwerk systemen bij inbraak alleen een lokaal aanvalspunt en eventueel direct verbonden stations gevaar lopen. Dit is een bezwaar dat voor vele gezondheidsinfrastructuur geldt zoals bijvoorbeeld het LSP en het XDS-systeem (beelduitwisseling), maar ook voor Zorgdomein en knooppunten voor werk en inkomen en het gemeentelijk domein. Een netwerk-oplossing is by design minder risicovol dan een “fietswiel” oplossing. De belangrijke principes van dataminimalisatie en scheiding zijn afgedekt in de netwerk oplossing terwijl het fietswiel overmatig gebruik bijna uitlokt en dus allerlei nieuwe vereisten meebrengt om dit te voorkomen

9 https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/02/08/kamerbriefover-versleuteling-gegevens-lsp/kamerbrief-over-versleuteling-gegevens-lsp.pdf

10 https://www.zorgictzorgen.nl/sterk-wisselende-betrouwbaarheid-medicatieoverzicht-lsp/

11 https://www.zorgictzorgen.nl/groot-traag-duur-en-vol-lucht-lsp-2/ en https://www.zorgictzorgen.nl/onbeschaamde-stimulering-lsp-functionaliteit-met-overheidsgeld-in-twinproject/

12https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/med/med_20110816_zienswijze_nictiz_epd.pdf

13https://www.nictiz.nl/wp-content/uploads/2018/06/PBLQ_Rapport-Gespecificeerde-toestemming.pdf

14 Verslag kamer debat januari 2019

15https://www.privacybarometer.nl/nieuws/3935/Wet_uitwisselen_medische_gegevens_via_LSP_onuitvoerbaar

16 https://www.nictiz.nl/wp-content/uploads/2018/04/Onderzoek_zorginfrastructuur.pdf17 https://whiteboxsystems.nl/nieuws/pilot-whitebox-succesvol-afgerond

17 https://whiteboxsystems.nl/nieuws/pilot-whitebox-succesvol-afgerond

18 https://www.ronroozendaal.nl/blog/2019/11/verwarring-over-toestemming en https://www.ronroozendaal.nl/blog/2019/12/toestemming-een-bijdrage-aan-de-hoedanwel en

19 https://whiteboxsystems.nl/mblog/reactie-verwarring-toestemming en Zorgverzekeraars Nederland: Onderzoek Whitebox; eindrapport 28 oktober 2019, door “We Do Trust” the technology governance company. Rapport in opdracht van Zorgverzekeraars Nederland.

20 https://nuts.nl/

21 Jacobs (2009) Architecture is politics: http://www.cs.ru.nl/~bart/PAPERS/cpdp09-jacobs.pdf

22 https://ibestuur.nl/weblog/wet-do-achterhaald-en-nodeloos-duur

23 NICTIZ (2017) Onderzoek zorginfrastructuur, 28 februari 2017, J.L van Duivenbode, Nictiz, The Netherlands.

24 De Vos (2020) ZorgICT en privacy by design. In voorbereiding

25 Dat dit niet denkbeeldig is geld bijvoorbeeld voor het gebruik van ROMmen en DBCs in de GGZ.

26 Hoepman (2020) https://www.cs.ru.nl/~jhh/publications/pds-boekje.pdf

27 https://privacybydesign.foundation/pdf/eherkenning-pbdf-maart20.pdf en
https://www.tno.nl/nl/aandachtsgebieden/informatie-communicatie-technologie/roadmaps/trustedict/
quantum/trusttester-veilig-valideren-van-persoonlijke-gegevens/

28 Projectvoorstel voor monitoring Kwaliteitskader GGZ, september 2018. UMCU, Van Os en de Vos. Inclusief verslag van pilotproject voor Nieuwegein.

29 Business Case, Conceptuele Architectuur, en Juridisch Kader (Centrale) Voorziening Datamanagement. juni 2019 Miles Ahead; in opdracht van Promedico, CGM & Portavita

30 Brief CBP aan VWS. Wijziging Ziekenfondswet en AWBZ. dd. 10 februari 2004 z2003-1433.

31 https://privacybydesign.foundation/irma/

32 De Vos (2018) De ontwikkeling van de ICT Gegevens-infrastructuur van de Overheid in relatie tot de 3 Gemeentelijke Decentralisaties in het Sociaal Domein: 15

33 Enabling Personalized Interventions, UvA, September 2017 NWO-project Person2Data.

34 https://www.dtls.nl/fair-data/personal-health-train/