Precisiegeneeskunde vereist privacy-bewaking EN een zeer lange adem

Precisie-geneeskunde en big-data-analyse van zorggegevens hebben veel met elkaar te maken. Een bedrijf als Philips, dat afscheid nam van beeldschermen en gloeilampen, zet thans vol in op deze doelen. Onder precisie-geneeskunde wordt de afstemming verstaan van een medische behandeling op de individuele kenmerken van elke patiënt. Men zoekt erbij naar de mogelijkheid om personen in subpopulaties te classificeren en dan gerichte therapie op die subpopulaties en liefst specifiek op een individuele patiënt te kunnen toepassen. Het doel is om geneesmiddelen en therapieën te vinden die uniek toepasbaar zijn op individuele patiënten, gebaseerd op genetisch onderzoek en andere relevante informatie over de gezondheid van dat individu. In de oncologie kennen we al vormen van precisie-geneeskunde, bijv. bij sommige vormen van borstkanker, maar ook bij bepaalde vormen van leukemie. Door o.a. genetisch onderzoek zijn subpopulaties te identificeren, waarbij bepaalde therapievormen kansrijk zijn. Ook kan voorkomen worden dat patiënten met een beperkte therapiegevoeligheid blootgesteld worden aan bij hen niet werkende (chemo)therapie. President Obama van de Verenigde Staten kondigde in 2015 in de State of the Union het ambitieuze Precision Medicine Initiative aan, een grootscheeps

onderzoek met grote inzet van mensen en middelen, waarbij naast het genoom van de betrokken patiënten ook gegevens van hun “lifestyle” bekeken worden. In een recente publicatie op 18 juli 2016 in een online magazine van het gezaghebbende Massachusetts Institute of Technology, de MIT Technology Review, stelt de research editor Mike Orcutt, dat het nog vele jaren gaat duren voor ook maar een deel van de gestelde doelen gehaald zullen worden. Ook anderszins zijn er signalen, dat alleen al op theoretische gronden genoomonderzoek zijn beperkingen kent. Daarnaast zijn er grote consequenties op privacy-gebied aan het verzamelen van DNA-informatie op grote schaal.

MIT

In het artikel in de MIT Technology Review worden een viertal punten aangestipt die duidelijk maken dat de weg die te gaan is nog lang zal zijn.

- De wetenschap rond genoom-afwijkingen is nog jong. Honderden genetische afwijkingen bij kwaadaardige tumoren, maar ook bij diabetes en hartziekten zijn ontdekt, maar veel is nog onbekend over wat die afwijkingen medisch gezien betekenen.
- Precisiegeneeskunde vereist bij onderzoeken van het genoom diepgaande en betrouwbare genetische testen. De testen die op de markt zijn gekomen zijn niet allemaal even betrouwbaar. “Different tests can produce different results from the same DNA sample, says Elizabeth Mansfield, the deputy director of personalized medicine and molecular genetics for the FDA.”
- Het zeer uitgebreide DNA-onderzoek is wel mogelijk maar erg kostbaar. Helemaal, als dat op grote schaal gebeurt. Als daarnaast ook een specifiek medicijn ontwikkelt moet worden(“targeted drug”) voor een beperkte groep patiënten zal dat nog veel meer financiële offers vragen.

- Het aantal mensen waarvan tot nu toe de benodigde data zijn verkregen is nog veel te laag om uitgebreide conclusies toe te laten.

Oxford

Begin mei 2016 sprak professor Gillies McKenna van het Department of Oncology van de Universiteit van Oxford op een congres in Maleisië over precisiegeneeskunde. Hij stelde dat in zijn vakgebied, de oncologie, de precisiegeneeskunde het meest gehypet is. McKenna voorziet een lange weg die afgelegd moet worden voor betekenisvolle vorderingen gemaakt worden. Hij maakte bijvoorbeeld duidelijk dat zelfs als er relevante genetische eigenschappen gevonden worden, die specifiek zijn voor een bepaalde tumor, deze tijdens het doorgroeien van de maligniteit ook weer kunnen muteren. Daardoor is wat je op moment A weet, op moment B weer achterhaald. Het vinden van enige therapie wordt daardoor zeer lastig.

Privacy

Het Precision Medicine Initiative in de V.S. wordt uitgewerkt in het Precision Medicine Cohort Program. Het doel is binnen drie a vier jaar een miljoen Amerikaanse vrijwilligers te vinden, die bereid zijn hun genoom te laten ontrafelen en hun leef-/gezondheidzorgdata te delen. Liefst wil men meer dan een miljoen deelnemers. Het Witte Huis stelde een zeer uitgebreid protocol op voor de veiligheid van de data en de privacy voor de deelnemers. Wil men op voorhand het vertrouwen van de burgers in een dergelijk project hebben en dat zo houden, dan is het noodzakelijk een dergelijk zeer uitgebreid protocol op te stellen en voorzorgen te nemen. Het document is opgesteld na uitgebreide consultaties van veel overheidsinstellingen en organisaties. Waarschijnlijk zal er best nog het nodige op aan te merken zijn door fijnproevers op het gebied van privacy in de zorg, maar het is tenminste een serieuze aanzet, al was het maar om de discussie bij massaal DNA-onderzoek op gang te krijgen.

Nederland

De precisie-geneeskunde als denkmodel gaat Nederland niet voorbij. In ons land zie je op dit moment sluipend een verdienmodel ontplooit worden waarmee op basis van grote hoeveelheden zorgdata precisie-geneeskunde-onderzoek en de daarmee samenhangende big-data-analyse uitgevoerd gaat worden. Het betreft voornamelijk bilaterale contracten tussen bijv. Philips en SurfSara, maar ook tussen Philips en het Radboud Universitair Medisch Centrum. Duidelijkheid over de toestemming van de patiënt voor het gebruik van de data, over het dataverkeer en de privacy van de patiënt dient gegarandeerd te zijn. Nergens zijn nog uitgebreide beveiligings- en privacy-protocollen geopenbaard en besproken. Het "vrijwillig" laten analyseren van DNA-materiaal heeft voor betrokkenen grote consequenties. Al was het alleen maar bij het aangaan van levensverzekeringen, bijvoorbeeld bij het afsluiten van een hypotheek. Wat moet men in zo'n geval invullen, wanneer bij de keuring gevraagd wordt of er sprake is van een erfelijke ziekte en of onderzoek van erfelijk materiaal verricht is? Een "ja" leidt tot verdere vragen en tenslotte weigering de verzekering af te sluiten.

Het sluipend starten van samenwerkingsverbanden zonder voldoende openbare aandacht voor privacy en datasecurity is geen goede zaak.

W.J. Jongejan

Hoogleraar informatiebeveiliging acht opzet LSP achterhaald en onveilig

Op 5 april j.l. heeft de vaste Eerste Kamercommissie voor VWS een twee uur durend gesprek gevoerd met deskundigen over cliëntenrechten bij elektronische verwerking van gegevens. Het ging over de kansen en risico's van de invoering van het wetsvoorstel 33509. Dit wetsvoorstel poogt de elektronische medische datacommunicatie een wettelijk fundament te geven. Het lijkt te gaan om alle vormen van die datacommunicatie, maar is volledig toegesneden op het gebruik van het Landelijk SchakelPunt(LSP). De inbreng van professor Eric Verheul, hoogleraar bij de Digital Security Group van de Radboud Universiteit van Nijmegen, was uitermate helder. Hij stelde in zijn betoog, dat de opzet van het LSP thans volledig achterhaald is. De huidige opzet beschouwt hij als kwetsbaar. De kern van het systeem acht hij onwenselijk en technisch niet noodzakelijk. Hij is niet zomaar iemand die dit zegt, maar een wiskundige met veel kennis van zaken betreffende cryptografie en veiligheidsmanagement op ICT-gebied.

Verslag

Deze week werd op de website van de Eerste Kamer het verslag van het deskundigengesprek gepubliceerd. Op pagina 18 en 19

staat de bijdrage van professor Verheul. Bij het LSP maakt binnen de centrale computer gebruik van een verwijsindex waarin bijgehouden waar van een bepaalde burger(specifiek burgerservicenummer) medische gegevens zijn vastgelegd en opvraagbaar zijn. Hij zegt daarover:

“Dat is eigenlijk heel grote tabel in een centraal systeem. Je kunt het zien als een grote matrix, waarbij op de rijen de bsn-nummers van de gebruikers staan. De wet voorziet erin dat er toestemming wordt gegeven voor het gebruik van het bsn. In de kolommen staan de zorgaanbieders. Je kunt je voorstellen dat waar beide elkaar kruisen, staat: deze man of vrouw is patiënt bij deze zorgaanbieder. Zo’n verwijsindex wordt eigenlijk impliciet genoemd in het wetsvoorstel. Dat is een heel gevoelige tabel, die onwenselijk en technisch gezien niet noodzakelijk is. Dat is het belangrijkste punt dat ik wil maken. In eerdere besprekingen van landelijke schakelpunten is al naar voren gekomen waarom het onwenselijk is. Als zo’n tabel in verkeerde handen valt, is plots duidelijk wie waar patiënt is. Het kan ook om een hiv-kliniek of een ggz-instelling gaan. Daarom wil je een centraal systeem met zo’n verwijsindex vermijden. Het is een heel grote tabel die heel lastig te beveiligen is. Het is technisch gezien niet noodzakelijk en dat biedt een perspectief dat in het verleden niet echt is besproken of bekeken.”

Anders

Hij geeft ook aan dat het anders kan:

“In 2014 hebben we allerlei cryptografische technieken ontwikkeld om de privacy binnen zo’n eID-stelsel te beschermen. De technieken die in 2014 zijn ontwikkeld, zou je relatief gemakkelijk kunnen toepassen in verwijsindexen die volledig gepseudonimiseerd zijn. De functionaliteit van de systemen van VZVZ en de gespecificeerde toestemming kun je daarin regelen, maar je houdt wel een systeem over dat veel cleaner is, omdat er geen persoonsgegevens maar pseudoniemen

in worden verwerkt.”

Zijn opmerkingen laten niets aan duidelijkheid te wensen over.

Niet van deze tijd

Al enige tijd terug werd duidelijk dat informatie die via het LSP getransporteerd wordt, korte tijd zich onversleuteld in de centrale computer bevindt. Bij alle gelegenheden waarbij kritiek op die manier van werken wordt geuit, bestrijdt VZVZ altijd dat dit een veiligheidsissue is. Professor Verheul stelt hierover:

“Die gegevens worden versleuteld verstuurd naar het LSP, zeg maar de hub, de centrale spil. Ze worden daar ontsleuteld en vervolgens opnieuw versleuteld naar de opvragende zorgaanbieder verstuurd. Dat is een manier van werken die tien jaar geleden, toen dit soort systemen werd ontwikkeld, misschien nog wel logisch was, maar op dit moment is het niet meer gebruikelijk dat gegevens eventjes in the clear, onversleuteld, in zo’n centraal systeem staan. Met het eID kun je met een bankmiddel, bijvoorbeeld een bankpas van de ING, inloggen bij de Belastingdienst. Uiteindelijk krijgt dan de Belastingdienst het bsn van de gebruiker, maar dat bsn staat op geen enkel moment eventjes in plain text op de systemen van de ING. Die oude manier van werken, waarbij die versleuteling even ongedaan wordt gemaakt op een centrale plek, is niet meer van deze tijd”

Gehakt

Het moge duidelijk zijn dat professor Verheul met deze uitspraken gehakt maakt van de huidige opzet van het LSP. Zowel de opzet van de centrale verwijsindex als de ontsleuteling van data, die de centrale computer passeren, acht hij niet meer van deze tijd. Het zijn waarschuwende woorden uit onverdachte hoek. Het wordt tijd dat de politiek die ter harte neemt, maar ook dat de zorgkoepels die nu nog in VZVZ meebeslissen over het LSP hun verantwoordelijkheid nemen.

W.J. Jongejan