

Zes voorwaarden voor het pse

Auteur: Jaap van der Wel
Illustratie: Arend van Dam

Met het groeien van de informatie-uitwisseling in de medische sector groeit het risico van 'collateral privacy damage'. Het versleutelen van gegevens kan dit voorkomen.

Rond afscherming van medische gegevens ontwikkelt zich een paradoxale situatie. Deze gegevens zijn vertrouwelijk maar worden steeds vaker en op steeds grotere schaal uitgewisseld. Dit begon in de jaren tachtig met ziekenhuisautomatisering en koppelen van bestanden binnen waarnemgroepen van huisartsen of samenwerkingsverbanden van apothekers. In de tussentijd zijn daar vele onderzoekers en statistiekmakers bij gekomen zoals het Centraal Bureau voor de Statistiek en ook beslissers zoals de centrale indicatieorganen.

Binnenkort wordt daar het elektronisch patiëntendossier (EPD) aan toegevoegd evenals het elektronisch kinddossier (EKD). Een goede volgende kandidaat is de uitwisseling van DNA-gegevens die een steeds belangrijkere rol gaan spelen bij onder meer oncologie.

Met het groeien van de informatie-uitwisseling tussen medici, groeit ook de 'collateral privacy damage' bij de ontwikkeling en het beheer van de uitdijende ict. Zo wordt in de praktijk vaak getest met productiegegevens waardoor testverslagen met vertrouwelijke gegevens rondslingeren op de bureaus van de it'ers. Verder hebben de systeembeheerders van softwareleveranciers vaak inzage in patiëntgegevens. Met versleuteling van databases of andere oplossingen dit vaak wel tegengegaan maar als softwarestoringen verholpen moeten worden, dan is toch inzage nodig in de onversleutelde gegevens om na te gaan hoe de storing is ontstaan.

Bij een nieuw plan voor inzage in medische gegevens stelt de bedenker natuurlijk de voordelen voorop en acht gewoonlijk de privacy nadelen acceptabel. De optelsom van al die plannen leidt er echter toe dat vertrouwelijke medische gegevens beginnen door te dringen tot de top van de gegevens die het meest worden rondgepompt in ons land. De pleidooien van privacyaanhangers tegen

het landelijk EPD en andere uitbreidingen zijn begrijpelijk. Ze maken echter geen schijn van kans zoals het verleden heeft laten zien: de controlebehoefte van bestuurders wint het keer op keer. Een mijlpaal voor groot-schalige administraties was de bevolkings-administratie die Napoleon tegen veel weerstand in realiseerde om met dienstplicht zijn veroveringslegers op te bouwen. De motieven van de huidige controlebehoefte, zoals het voorkomen van ongelukken met geneesmiddelen, zijn natuurlijk nobeler dan toen. Niettemin is de tendens onmiskenbaar: gegevensuitwisseling wordt steeds grootschaliger en intensiever. Er zijn creatievere oplossingen nodig dan tegenhouden.

Vingerafdruk

Een voorbeeld van een creatieve oplossing is de methadonverstrekking aan drugsverslaafden. Instellingen voor gezondheidszorg kunnen drugsverslaafden voordragen. Om de verstrekking te controleren, worden de gegevens van die patiënten voorzien van een versleuteld kenmerk dat is afgeleid uit de vingerafdruk van de patiënt en opgeslagen in een landelijke database.

Een drugsverslaafde die zich meldt bij het distributiepunt voor zijn onderhoudsportie methadon, identificeert zich met zijn vingerafdruk waarop die vertaald wordt naar de sleutel waarmee de gegevens worden opgezocht in de landelijke database. Het resultaat is een strak systeem van methadonverstrekking waardoor verslaafden niet op één dag in verschillende steden een portie kunnen ophalen. De gegevens in de landelijke database zijn anoniem maar bieden wel de mogelijkheid om een drugsverslaafde aan zijn gegevens te koppelen.

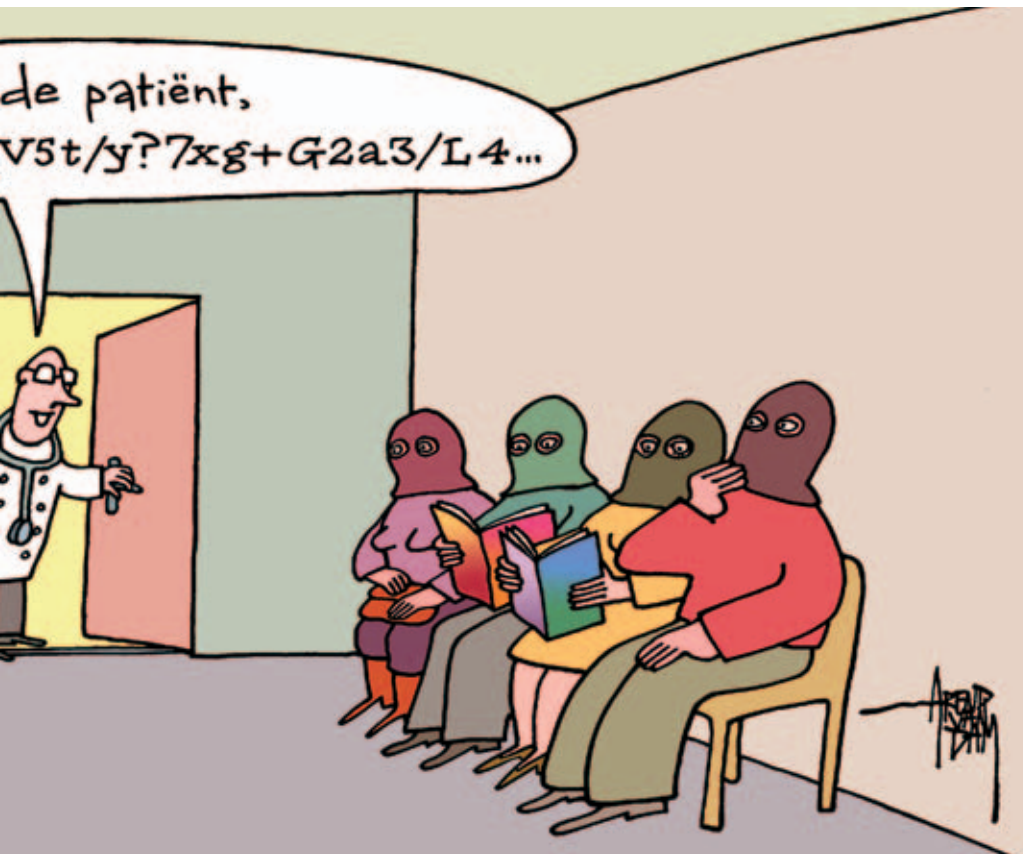
Een ander voorbeeld dat in ontwikkelstadium verkeert, is het project Parelsnoer waarmee universitaire gezondheidscentra medische gegevens willen samenvoegen voor weten-



schappelijk onderzoek. Een gezondheidscentrum versleutelt daarbij de identificerende gegevens, een centrale instelling verzamelt deze gegevens en voegt deze samen. Zo ontstaan meer onderzoeksmogelijkheden zonder de privacy van patiënten te schaden. Het voorgaande zijn voorbeelden van 'pseudonimiseren', een proces waarbij door versleuteling gegevens niet meer te herleiden zijn naar 'een geïdentificeerde of identificeerbare natuurlijke persoon' (formulering Wet bescherming persoonsgegevens). Die versleuteling wordt zo uitgevoerd dat de gegevens van dezelfde persoon onderling wel gekoppeld kunnen worden. Een goede oplossing voor pseudonimiseren voldoet aan zes voorwaarden.

De eerste ligt voor de hand: de versleuteling en ontsleuteling mag alleen worden uitgevoerd door de instantie die de vertrouwelijke gegevens ter beschikking stelt. Eventueel kan dit aan een gespecialiseerd bedrijf worden uitbesteed, een Trusted Third Party voor versleutelingsdiensten die versleuteling

udonimiseren van gegevens



een privacy audit kunnen hiervoor oplossingen worden ontwikkeld zoals het weglaten van gegevens die er niet toe doen, of postcodes te ontdoen van letters waardoor de plaatsaanduiding wordt vergroot. Hierdoor wordt het herleiden van gegevens naar personen gewoonlijk wel bemoeilijkt maar niet altijd onmogelijk of in de toekomst mogelijk door nieuw inzicht in de versleutelingsaanpak of snellere computers. Daarom is het als vijfde voorwaarde noodzakelijk dat de gegevensleverancier de ontvanger verplicht om gegevens alleen te gebruiken voor het doel waarvoor die zijn verstrekt, niet door te geven of zelf te combineren met andere persoonsgegevens en na bepaalde tijd te vernietigen of dat te doen op het eerste verzoek van de gegevensverstrekker als onverhoopt blijkt dat er bij het versleutelen iets mis is gegaan. In dat laatste geval kan de gegevensverstrekker de gegevens opnieuw leveren met een nieuwe codering. Als extra kan een gegevensverstrekker ervoor zorgen de versleuteling verschilt per gegevensafnemer, waardoor het voor gegevensontvangers lastig of onmogelijk wordt om gegevens te combineren.

Als zesde en laatste eis is aandacht nodig voor de informatie die ontstaat door het samenvoegen. Bij het EKD bijvoorbeeld wil men bevindingen van school, politie, buurt via de beschreven pseudonimisatieprocedure combineren. Wie beslist echter over ontsluiting en in en welke situatie rechtvaardigt de situatie het doorbreken van de privacy? Dit vraagstuk doet zich voor bij iedere samenvoeging van gepseudonimiseerde gegevens. De oplossing is een stevige, goed geregelde bevoegdheid en beslissers met voldoende inzicht in de reikwijdte van hun beslissingen. De zes eisen zijn niet ingewikkeld voor moderne informatietechnologie. Bij iedere overdracht van informatie naar instanties buiten de zorgverlener zouden deze oplossing standaard moeten worden ingezet. <

Jaap van der Wel is managing partner van Comfort-IA

Meer over informatiebeveiliging:
www.ictzorg.com/informatiebeveiliging

geheim houdt en geen gegevens bewaard. De tweede voorwaarde is wat in de literatuur het tweede desideratum van onze landgenoot Kerckhoff heet: de sleutel bevat het geheim, niet de manier van berekenen of constructie van de versleutelingsapparatuur want die valt vroeg of laat toch wel in handen van de vijand. Veranderen van een sleutel is eenvoudig maar veranderen van alle apparatuur is een kostbare grap. Kerckhoff formuleerde het principe in 1883 en het is nog steeds actueel zoals bleek toen het versleutelingsalgoritme van de OV-chipcard openbaar werd. Een belangrijk deel van het geheim bleek in het algoritme verstopt en na openbaar worden daarvan stelde de geheimhouding van de OV-chipcard weinig meer voor. Beter versleuteling kan maar vereist andere controlepunten wat erg kostbaar is. Gepubliceerde algoritmen die vele jaren internationaal wetenschappelijk zijn onderzocht in combinatie met een geheime, makkelijk aan te passen sleutel is dan beter. Voor het gehele proces van pseudo-

nimiseren geldt hetzelfde: dat moet zijn gedocumenteerd, gepubliceerd en getoetst door een deskundige die thuis is in de rekenkundige en de juridische kanten van het vraagstuk.

De derde voorwaarde is dat het algoritme onoverkomelijk veel rekenwerk moet vergen om het te kraken. Bij de huidige computersnelheid geldt als vuistregel dat het algoritme voldoende sterk is als er een getal met 1 met minimaal 40 nullen aan berekeningen is vereist. Maar tweemaal zo veel nullen is wenselijker en goed mogelijk. Om gelijke tred te houden met de toenemende rekensnelheid van computers moet de sterkte ook eenvoudig opgevoerd kunnen worden.

Als vierde voorwaarde is aandacht vereist voor de indirect identificerende gegevens. Zo maken postcode, huisnummer, geboortedatum en het inkomen op de cent nauwkeurig al snel identificatie mogelijk als men als men via andere weg ook over dergelijke gegevens beschikt. Met een statistisch analyse of