Platform voor kwaliteit van de organisatie

NEN-7524 versterkt privacy bij onderzoek met patiëntendata

14 oktober 2019 door Loek Kusiak

De norm NEN-7524, die onlangs is gepubliceerd, moet de vertrouwelijkheid in het gebruik van patiëntgegevens in onder meer medisch onderzoek vergroten. Data worden *gepseudonimiseerd*. Een beveiligingsmaatregel waarbij persoonsgegevens worden verwerkt, zonder dat daarbij duidelijk wordt om welke persoon het gaat. Een *trusted third party*, ofwel een onafhankelijke dienstverlener, verwijdert de oorspronkelijke gegevens en maakt hier een cryptocode van.

Patiëntgegevens vormen belangrijke bronnen voor medisch onderzoek en statistische input voor het ontwikkelen van gezondheidsbeleid door de overheid en maatregelen binnen ziekenhuizen en andere zorginstellingen. Voor onderzoekers en epidemiologen zijn patiëntgegevens interessant, bijvoorbeeld om trends te bepalen hoe vaak een ziekte op een bepaald moment onder een bepaalde populatie voorkomt (ziekteprevalentie), of om het effect van gezondheidsprogramma's te monitoren. Als gevolg van de wet AVG (Algemene Verordening Gegevensbescherming) luistert ook het waarborgen van privacy binnen medisch onderzoek steeds nauwer. Om zorggegevens ethisch en wettelijk verantwoord voor onderzoek te mogen gebruiken, worden de gegevens gepseudonimiseerd, een methode waarbij een algoritme de patiëntgegevens vervangt door versleutelde gegevens: het pseudoniem.

> *Om zorggegevens ethisch en wettelijk verantwoord voor onderzoek te mogen gebruiken, worden de gegevens gepseudonimiseerd, een methode waarbij een algoritme de patiëntgegevens vervangt door versleutelde gegevens: het pseudoniem.*

Betrouwbaarheid verbeteren

In de AVG staat dat pseudonimisatie nuttig is en organisaties 'technische en organisatorische maatregelen' moeten nemen. Dit betekent dat een vertrouwde onafhankelijke partij – een *trusted thrid party* – de gegevens verwijdert die herleidbaar zijn tot de patiënt en vervangt door een pseudo- of cryptocode.

Voor de dienstverlening ten aanzien van pseudonimisatie heeft NEN in juli 2019 de Nederlandse norm NEN 7524 gepubliceerd. Het doel van de norm is de privacy van de patiënten te respecteren en de beschikbaarheid van de gegevens over langere tijd veilig te stellen.

'Tegelijkertijd moet de norm ook de transparantie en betrouwbaarheid van pseudonimisatiediensten verbeteren,' zegt Marlou Bijlsma, standaardisatie consultant healthcare bij NEN. De NEN-norm is een Nederlandse variant als aanvulling op de internationale norm ISO 25237, waarin de verschillende vormen van pseudonimisatie staan opgesomd.

Trusted third party

Bijlsma: 'Neem bijvoorbeeld een universiteit die onderzoek heeft gedaan naar diabetes, maar ook onderzoek doet naar hoge bloeddruk en hart- en vaatziekten. Een onderzoeksvraag kan dan zijn welke patiënten zowel diabetes als hoge bloeddruk of hart- en vaatziekte hebben. De onderzoekers werken dan met gepseudonimiseerde datasets van deze patiënten, die met het onderzoek hebben ingestemd. De datasets kunnen worden gekoppeld, nog steeds zonder dat de privacy in het geding komt.'

Het ICT-bedrijf dat als onafhankelijke partij diensten op het gebied van pseudonimisatie verleent, zorgt er met een cryptocode voor dat de gegevens van patiënten op gepseudonimiseerde wijze aan onderzoekers worden doorgegeven, bijvoorbeeld door aan een persoon steeds hetzelfde pseudoniem toekennen: 'Hans' is nummer *1 (#(0) (votgujp)* 'Piet' is nummer 2, enzovoort. Daardoor kunnen dienstverleners informatie uit verschillende bronnen kunnen combineren maar op verzoek van onderzoekers ok nieuwe informatie toevoegen.

Bijlsma: 'Je kan met data dus heel veel doen, maar dan moet je wel goed regelen dat de privacy beschermd wordt, onder meer tegen ongeautoriseerd inloggen en slordig gebruik. De NEN-norm geeft daar de handvatten voor.'

Connecties leggen

Pseudonomiseren is voor onderzoekers veel interessanter dan anonimiseren, een techniek van *data-masking* waarbij alle persoonsgegevens worden uitgewist. Achternamen kunnen bijvoorbeeld worden verwisseld. Bepaalde gegevens, zoals de eerste cijfers van een nummer, kunnen worden gewist waardoor gegevens ook in geen enkele vorm meer te gebruiken zijn wanneer de onderzoeker op een hoger niveau de relatie wil leggen tussen patiënten met diabetes en patiënten met hoge bloeddruk.

> *Pseudonomiseren is voor onderzoekers interessanter dan anonimiseren, een techniek van data-masking waarbij alle persoonsgegevens worden uitgewist.*

Bijlsma: 'Met gegevens die gepseudonimiseerd zijn, zijn wel verbanden te leggen tussen aandoeningen en/of patiëntenpopulaties. De data dat iemand diabetes heeft en daarnaast medicijnen gebruikt, blijven aan elkaar gekoppeld, maar zijn niet naar een persoon herleidbaar.'

Dit type data levert dan ook weer statistische gegevens op voor bijvoorbeeld het RIVM dat uitspraken doet over de gezondheidssituatie van Nederlanders. Ook zorgverzekeraars gebruiken gepseudonimiseerde data om beleid te bepalen

voor verzekerbare zorg voor klanten, bijvoorbeeld over de effectiviteit van medicijnen.

‘Absolute maatregel’

Met behulp van het algoritme kan de versleuteling van patiëntendata ook weer worden teruggedraaid. Omdat het versleutelingsproces zogezegd ‘omkeerbaar’ is, zijn gepseudonimiseerde data over een identificeerbare persoon nog steeds persoonsgegevens die herleidbaar zijn als onderzoekers aanvullende gegevens blijven toevoegen.

‘Wanneer je data over individuen verzamelt, kun je stellen dat je persoonsgegevens aan het verzamelen bent, wat de reden is waarom de AVG vereist dat je alleen de data gebruikt die voor je onderzoek nodig zijn,’ zegt Hans van Vlaanderen, directeur van pseudonimisatiedienstverlener Stichting Zorg TTP (Trusted Third Party), dat ook bij de opstelling van de NEN-norm betrokken is geweest.

> *“ Gepseudonimiseerde informatie is alleen tot personen te herleiden als het toegepaste algoritme bekend is.*

‘Pseudonimisering is daarmee ook een ‘absolute maatregel’ die de kans vermindert op misbruik van gegevens bij datalekken in de zorg, die nog vaak voorkomen’, stelt Van Vlaanderen. ‘Immers, gepseudonimiseerde informatie is alleen tot personen te herleiden als het toegepaste algoritme bekend is.’

Eerst halffabrikaat

Hoe werkt het precies? Stichting Zorg TTP neemt de dataset, patiëntgegevens dus, in ontvangst van bijvoorbeeld een ziekenhuis waar Zorg TTP software heeft geïnstalleerd. Van Vlaanderen: ‘Namen en BSN-nummers in deze dataset worden eerst vervangen door een halffabrikaat pseudoniem. De tweede stap vindt plaats in onze centrale verwerkingsomgeving waar het definitieve pseudoniem wordt toegevoegd. Identiteitsgegevens worden omgezet in, simpel gezegd, bijvoorbeeld ‘1,2 of 3′ of’ ‘A, B of C’. Wij zorgen ook voor een veilig transport van deze data.’

Behalve voor ziekenhuizen pseudonimiseert Stichting Zorg TTP data voor aanbieders en/of afnemers zoals het Zorginstituut Nederland, het RIVM, de Nederlandse Zorgautoriteit, Nivel en de traumaregistratie van het Landelijk Netwerk Acute Zorg. Van Vlaanderen: ‘We krijgen wel de sleuteltjes, de data dus, in handen maar na bewerking beschikken we niet meer over het eindresultaat. Iedereen in de keten heeft elkaar nodig om tot gepseudonimiseerde data te komen en je bent volstrekt transparant over wat je doet en hoe je dat doet.’

Cloud Google

Met de opkomst van partijen als Google is inmiddels duidelijk geworden dat wie data heeft, daarmee macht en invloed kan uitoefenen – en ook ongewenste dingen kan doen. Zo kwam begin 2019 in de openbaarheid dat Google in de cloud van honderdduizenden ziekenhuisbezoekers de medische gegevens bewaart door tussenkomst van het bedrijf MRDM, dat zich presenteert als Trusted Third Party.

> *“ Met de opkomst van partijen als Google is inmiddels duidelijk geworden dat wie data heeft, daarmee macht en invloed kan uitoefenen – en ongewenste dingen kan doen.*

Ook Nederlandse ziekenhuizen nemen diensten af van MRDM, dat data opslaat in de cloud van Google. Ziekenhuizen wisten ervan, maar niet de patiënten. De informatie wordt verwerkt voor landelijke kwaliteitsregistraties en interne analyses voor ziekenhuizen, zodat ze ook elkaars prestaties kunnen vergelijken.

Voor de registratie van onder meer borstkanker krijgt MRDM gegevens over iemands behandeling. Dan gaat het om medicijngebruik, aantal ingrepen, complicaties en opnamedagen. De gegevens worden door ziekenhuizen uit het elektronisch patiëntendossier gehaald en naar MRDM gestuurd, die de naam van de patiënt vervangt door een nummer, pseudonimiseren dus.

Onrust

De opslag door MRDM van patiëntendata in de cloud bij Google riep bij Kamerleden en Nederlandse patiëntenfederaties wel kritische vragen op. Gebruikt Google de gegevens ergens voor? Zijn de patiëntgegevens daar wel veilig? Dat zijn ze, aldus de Autoriteit Persoonsgegevens (AP) die zich over de kwestie boog en besloot geen extra onderzoek te doen naar de verwerking van medische gegevens in de cloud van Google.

Volgens de AP voldoet databedrijf MRDM, dat vooraf de verplichte risicoanalyse heeft uitgevoerd, aan de vereisten voor bescherming van data van Europese burgers via het EU-US Privacy Shield-raamwerk, inzake de overdracht van persoonlijke gegevens van de EU naar Amerika. Omdat de gegevens in een Nederlands datacentrum staan (Eemshaven), vallen zij onder Nederlandse en Europese wet- en regelgeving.

Wel wil minister Bruins (Medische Zorg) nog weten of het wenselijk is – daar loopt onderzoek naar – dat de gegevens van honderdduizenden patiënten via verwerkers versleuteld bij niet EU-cloudbedrijven belanden. De minister daarover: 'Ik hecht bij de verwerking van medische gegevens het grootste belang aan privacybescherming en informatiebeveiliging.'

Kwaliteitssystemen

Hans van Vlaanderen van Stichting Zorg TTP gelooft niet dat controle door de AP op de wijze waarop in de praktijk uitvoering wordt gegeven op korte termijn al aan de orde is. 'Daarvoor is de norm nog te nieuw. Bovendien kennen we al de NEN-7510, die het hele gebied van informatiebeveiliging in de zorg dekt en niet beperkt blijft tot technische specificaties. Het gaat dan ook over de organisatie en het menselijk handelen, en daar hoort een kwaliteitszorg- en managementsysteem bij. Wat niet wil zeggen dat een check door de AP of een andere inspectiedienst naar de staat van informatiebeveiliging in de zorg maar achterwege moet blijven, integendeel.'

Bijlsma van NEN: 'Binnen de NEN-norm 7524 wordt ook verwezen naar het belang van systemen voor kwaliteits- en informatiebeveiliging. Maar in de AVG en andere regelgeving gaat nu eerst de aandacht uit naar zelfregulering en de boodschap dat je data moet pseudonimiseren en hoe je dat effectief doet. Ik denk dat de toetsing door de AP nog toekomstmuziek is. De AP richt zich nu vooral op datalekken, op onderzoek van incidenten.'

door Loek Kusiak, freelance journalist

Vorige

Risicoleiderschap in de praktijk: de advi…

Wat is risicoleiderschap en waarom is het nodig? Hoe werkt risicoleiderschap in de praktijk en welke … Read more

Categorie: Artikelen
Tags: data en kwaliteit, Gezondheidszorg, NEN 7524, privacy
Thema: Digitale transformatie, ISO Certificering

Geef een reactie

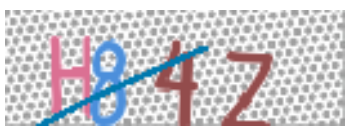
Het e-mailadres wordt niet gepubliceerd. Vereiste velden zijn gemarkeerd met *

Reactie

Naam *

E-mail *

Website



CAPTCHA code
*

REACTIE PLAATSEN

Deze website gebruikt Akismet om spam te verminderen. Bekijk hoe je reactie-gegevens worden verwerkt.

Zoeken

AANMELDEN NIEUWSBRIEF

ACTUELE DOSSIERS

De kwaliteitsfunctionaris als gangmaker?

Kritische kwaliteitskunde

ISO Certificering

Digitale transformatie

GERELATEERDE ARTIKELEN

14 mei 2019
Digitale infrastructuur voor medische kennis

2 mei 2019
Hoe bezieling werkt

3 april 2019
Kees Ahaus: 'Samenwerken is het nieuwe fuseren in de zorg'

19 december 2018
De nieuwe uitdaging voor kwaliteitsmanagement (2)

27 november 2018
Effecten van verbeterprogramma gemeten

30 oktober 2018
Kwaliteit en data: uitdaging voor kwaliteitsmanagement (deel 1)

16 mei 2018
Kwaliteitsexpert Don Berwick: Nieuw tijdperk van leren en verbeteren

8 maart 2018

Douwe Biesma: ‘Het gaat niet om zorgkwaliteit, maar om waarde voor de patiënt’

31 juli 2017

Lean kun je niet implementeren

11 juli 2017

Kwaliteitsnormen en keurmerken voor marktonderzoek

AGENDA

Jaarcongres Procesmanagement
27 november 2019

Collegereeks Kwaliteit in digitale transitie
Start 12 november 2019

En verder:

Collegereeks Circulaire Economie
Start 5 november 2019

Collegereeks Samenwerken in netwerken
Start 12 november 2019

Jaarcongres Transitiemanagement
21 november 2019

Jaarcongres Verandermanagement
6 december 2019

Event Verdraaide Organisaties
13 december 2019

Bekijk de gehele agenda hier

Voeg een nieuw agenda item toe

VACATURES

» Klik hier voor meer vacatures

PARTNERS