

Datarevolutie in de zorg: even kansrijk als urgent

Auteurs

Sarah van Drumpt
Marie Beth van Egmond
Joachim de Greeff
Mike de Roode
Rik Rurup
Alexander van den Wall Bake
Jildau Bouwman
André Boorsma

Een oproep voor
medische vooruitgang
door ethisch
datagebruik



Inhoudsopgave

Introductie	3
1. Wat als we ontoegankelijke data nu wél toegankelijk kunnen maken?	4
2. Gezonde zorgen over de datarevolutie	5
3. Vier doorbraaktechnologieën	6
Privacy Enhancing Technologies	6
Data Spaces	7
Self-Sovereign Identity	8
Generatieve AI	9
Conclusie	10

Introductie

De technologie en de wetgeving die nodig zijn om data op een veilige manier te ontsluiten staan op het punt om de zorg te veranderen. Een alternatief voor het huidige systeem, waarin onduidelijke grenzen en overmatige administratie de norm zijn, is eindelijk in zicht. Doeltreffendere coördinatie, volledige medische dossiers en geavanceerder onderzoek worden mogelijk. Daardoor kan ons zorgsysteem duurzamer, toegankelijker en betaalbaarder worden, met behoud van privacy en autonomie. Daarvoor is wel dringend actie nodig.

Een groeiend ecosysteem van start-ups heeft zich in de afgelopen jaren gestort op het beschikbaar en bruikbaar maken van technologieën als [Data spaces](#), [Privacy Enhancing Technologies](#) en [Self-sovereign identity](#). De resultaten die daarmee geboekt worden zijn niet te negeren. Gezondheidsdata kunnen op steeds grotere schaal veilig én ten volle worden benut. Ook nieuwe wetgeving maakt duidelijk dat de tijd van vrijblijvendheid

voorbij is. De technologische versnelling wordt niet alleen in goede banen geleid, maar zeker ook op grote schaal mogelijk gemaakt.

In Europa geldt sinds 2016 de Algemene Verordening Gegevensbescherming (AVG). De AVG beschermt persoonsgegevens binnen de Europese Unie en waarborgt het vrije verkeer van gegevens. In Nederland is sinds juli 2023 is de Wet Elektronische Gegevensuitwisseling in de Zorg (Wegiz) van kracht. De Wegiz verplicht zorgverleners om in bepaalde gevallen digitaal te communiceren en bevat afspraken over bevoegdheden en toegang om de privacy van patiënten en cliënten beter te waarborgen. Ten slotte komt de European Health Data Space (EHDS) eraan. In deze wet wordt vastgelegd dat burgers van de EU snel en makkelijk medische gegevens moeten kunnen uitwisselen en toegang moeten hebben tot hun gezondheidsdata. De EHDS biedt daarnaast een extra mogelijkheid voor veilig secundair datagebruik¹.

Nieuwe technologieën en nieuwe regels maken een datarevolutie in de zorg onafwendbaar. Het vergt echter nog een zeer grote inspanning om zorgaanbieders digitaal op één lijn te krijgen en veilige uitwisseling technisch op de rails te krijgen. De zorg moet als één geheel aan het werk om te zorgen dat niemand achterblijft. Vertrouwen in elkaar en de systemen moet worden teruggewonnen, onder andere met technologieën zoals Data spaces,

Privacy Enhancing Technologies en Self Sovereign Identity. Daarnaast moeten het publiek en de professionals vertrouwen krijgen in het opkomende Generative AI als gesprekspartner.

Hieronder zullen we ingaan op de potentie van het vernieuwde datagebruik, twijfels die gegevens delen met zich meebrengen en zullen we de genoemde technische oplossingen bespreken.

Zonder de uitdrukkelijke toestemming van een patiënt krijgen hulpverleners geen volledig inzicht in hun gezondheidsgegevens. Informatie die elders is opgeslagen, bijvoorbeeld bij een huisarts of psychiater, mag niet zomaar worden gedeeld. Met name in spoedgevallen kan dit leiden tot gevaarlijke situaties. Sinds 2022 mag daarom een ‘spoedsamenvatting’ worden opgesteld, maar dat ene levensreddende detail kan nog steeds ontbreken. Het risico dat een arts een verkeerde combinatie van medicijnen voorschrijft, blijft onaanvaardbaar hoog². Ook als er geen spoed is.

Het is exemplarisch voor het gehele Nederlandse zorgsysteem: iedereen beschikt over een stukje van de puzzel, maar niemand heeft het hele verhaal. Dat is niet zonder reden. Het inzien, analyseren en delen van gezondheidsdata kan alleen als de privacy gewaarborgd blijft.

In dit paper betogen wij dat dit beter mogelijk is dan ooit tevoren. Dankzij meerdere doorbraakinnovaties ligt de weg open voor medische vooruitgang door ethisch datagebruik. Een datarevolutie is op handen. De spelers in het Nederlandse zorgsysteem staan voor de urgente opdracht om haar kansen te benutten.

¹ Data gebruik voor wetenschappelijk onderzoek, innovatie, beleidsvorming, patiëntveiligheid, gepersonaliseerde geneeskunde, officiële statistieken en/of regelgeving. En zie: <https://www.gegevensuitwisselingindezorg.nl/european-health-data-space-ehds>

² 'Wissel medicatiegegevens patiënten standaard uit, tenzij bezwaar' (nos.nl)

1. Wat als we ontoegankelijke data nu wél toegankelijk kunnen maken?

De datarevolutie wordt gekenmerkt door explosieve groei, evolutie en impact van gegevensgebruik in alle aspecten van de samenleving en industrie. Bij uitstek in het domein van de zorg brengt dat ongekende kansen met zich mee. Niet alleen door gebruik van AI, maar juist door het samenbrengen van partijen die met data werken: op alle vlakken zijn grote verbeteringen mogelijk.

Hoe beter de uitwisseling van gegevens, hoe beter de zorg (-coördinatie). Voor de patiënten en cliënten leiden verbeterde data-inzichten tot de verlichting van stress en ongemak. Het is immers niet langer nodig om zelf dossiers mee te nemen en er kan niks vergeten worden in een intakegesprek. Voor behandelaars en instellingen dalen de kosten omdat er minder fouten worden gemaakt en minder dubbel werk gedaan wordt. Afspraken worden effectiever en patiënten komen sneller bij de juiste specialist terecht.

Een enorme vermindering van administratieve taken is mogelijk. Een cliënt of patiënt kan al op afstand begeleid worden. Bij diabetespatiënten kunnen artsen tegenwoordig bijvoorbeeld via slimme meters met de cliënt meekijken. Patiënten hoeven niet meer naar een consult te komen als het goed gaat.

De optie tot 'secundair datagebruik', voor bijvoorbeeld wetenschappelijk onderzoek, biedt grote kansen voor vernieuwing en verbetering doordat onderzoek beschikt over veel grotere populaties. Met behulp van data uit verschillende bronnen kunnen we sneller meer te weten komen over zeer zeldzame aandoeningen. Ook kan er beter naar lokale of regionale effecten gekeken worden, bijvoorbeeld door informatie over klachten aan gegevens over luchtvervuiling te koppelen. Deze multidimensionale data aanpak kan leiden tot grote verbeteringen in zorg, patiëntveiligheid en zelfs (preventie-)regelgeving.

De beloftes zijn groot, maar om deze kansen ten volste te benutten moet er nog veel gebeuren. We moeten de gezonde twijfels over privacy die voortkomen uit deze datarevolutie adresseren. Dat kan door nieuwe nationale en Europese ontwikkelingen op het gebied van regelgeving, nieuwe technieken, en voorbeelden uit andere sectoren te omarmen. Het wiel hoeft niet opnieuw uitgevonden te worden, maar wel toegepast. In hoofdstuk 2 gaan we in op veelgehoorde, terechte twijfels en in hoofdstuk 3 leggen we uit hoe die geadresseerd kunnen worden met nieuwe technologie.

2. Gezonde zorgen over de datarevolutie

Nieuwsberichten over data-lekken, ransomware aanvallen, hacks, privacy-schendingen en onethisch handelen van personeel zijn aan de orde van de dag. Gaan we niet te snel? Kan iedereen meekomen? Levert het écht minder werk op? Hoewel het begrijpelijk is dat het beschikbaar stellen van gevoelige data aan externe partijen weerstand oproept, mogen deze twijfels geen belemmering vormen om vooruitgang te boeken en dieper in te gaan op de laatste ontwikkelingen. Nieuwe technologieën, waaraan TNO bijdraagt met kennisontwikkeling, hebben de potentie om bezwaren weg te nemen. Het is belangrijk om deze samen uit te gaan proberen in bijvoorbeeld een pilot.

Dat er twijfels zijn over digitalisering of data (her)gebruik is begrijpelijk en soms ook terecht. In dit hoofdstuk adresseren wij vier van deze mogelijke zorgen: privacy, het vertrouwen in andere partijen, controle over gegevens en de rol van de mens in een digitale samenleving.

Niet voor niets is er een hoop wet- en regelgeving om de privacy van patiënten te beschermen, bijvoorbeeld de Algemene

verordening gegevensbescherming (AVG). Het combineren van data van twee ziekenhuizen zou een enorme bron van informatie opleveren, maar mag gelukkig niet zomaar. Met *Privacy-Enhancing Technologies* kan ervoor worden gezorgd dat deze bruikbare informatie wel kan worden gebruikt, maar dat de privacy van patiënten wordt gewaarborgd.

Daarnaast zijn er ook twijfels over het vertrouwen binnen de sector. Is het mogelijk om een compromis tussen alle zorgverleners & IT aanbieders te sluiten over de manier van data inzicht, te denken aan het format, het middel en de bijbehorende verantwoordelijkheden? Zijn belanghebbenden in staat om samen knopen door te hakken of verzanden zij in getouwtrek en lopen we straks achter de feiten aan? Het concept van *Data Spaces* zorgt ervoor dat de benodigde afspraken worden vastgelegd en dat elke partij controle houdt over zijn eigen data.

Ook kan er vanuit een patiënt het gevoel ontstaan dat je de controle verliest over je gegevens. Aan de ene kant weet je niet wie er precies toegang hebben tot jouw gegevens, aan de andere kant hebben

misschien weer niet de juiste artsen of instanties toegang tot jouw data. Ook moet je er maar op vertrouwen dat de gegevens die anderen over jou hebben ook echt kloppen; er zit immers geen echtheidskenmerk aan vast. Technieken binnen het domein van *Self-Sovereign Identity* zorgen ervoor dat jij bepaalt welke gegevens je met wie deelt zonder dat er iemand mee kan kijken.

Ten slotte is er vanuit de patiënten en zorgverleners niet alleen twijfel over inzicht in data, maar ook argwaan over de rol van de mens in een digitale samenleving. Mensen krijgen soms lastig inzicht in de “slimme” beslismethodes en kunnen er daardoor moeilijk vertrouwen in hebben. Is het wel wenselijk dat een algoritme beslissingen over leven en dood maakt? Welke overwegingen maakt de computer? Blijft er nog plek voor een menselijke afweging? Binnen het domein van *Generatieve AI* wordt onderzocht hoe een mens op natuurlijke wijze kan samenwerken met computers. Zo kan zowel de patiënt makkelijker omgaan met de digitalisering én de arts beter gebruik maken van behulpzame inzichten van een computer.

In het volgende hoofdstuk nemen wij een viertal technologische doorbraken onder de loep die de potentie hebben om bovengenoemde twijfels elk op hun manier adresseren. Wanneer deze innovaties op de juiste manier worden toegepast bieden zij ons zorgsysteem de mogelijkheid om de datarevolutie verantwoord in te richten en ten volle te benutten. Om dit voor elkaar te krijgen is het van belang om samen met de zorgpartijen te experimenteren met deze innovaties. Alleen door gezamenlijke inspanningen kunnen de innovaties zodanig worden ontworpen dat ze aansluiten bij de uiteenlopende belangen van de verschillende zorgpartijen en patiënten, die allemaal een schakel zijn in het systeem. Zo zullen deze innovaties ook in de praktijk grootschalig worden toegepast en de beoogde impact bereiken.

3. Vier doorbraaktechnologieën

In dit hoofdstuk worden vier doorbraaktechnologieën belicht, elk ontworpen om specifieke risico's te mitigeren en nieuwe deuren te openen. Hoewel elk op zichzelf kan worden toegepast, levert verder onderzoek naar hun gecombineerde praktische toepasbaarheid aanzienlijke meerwaarde.

Privacy Enhancing Technologies

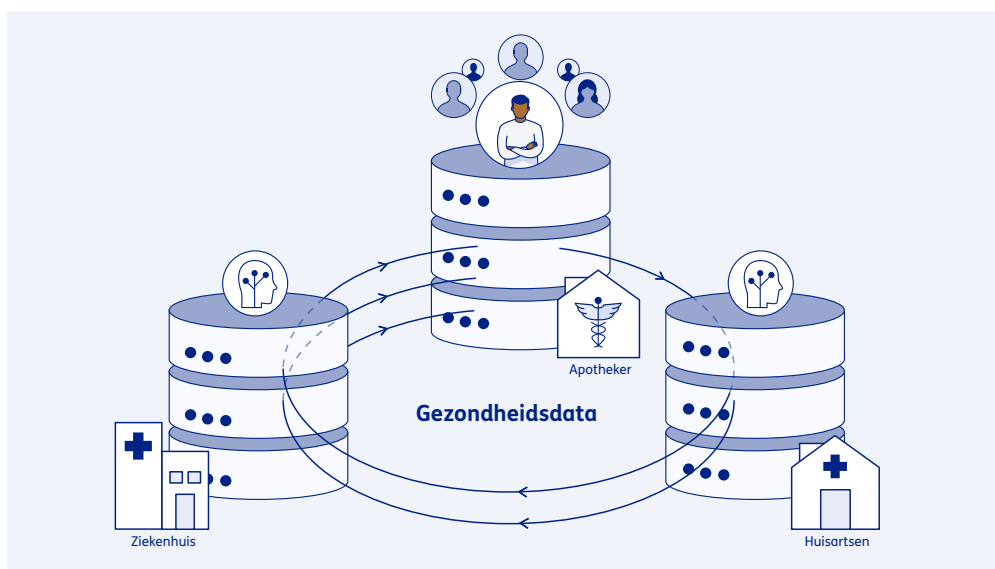
Wanneer meerdere partijen gegevens willen delen voor het verkrijgen van

nieuwe inzichten, bieden Privacy Enhancing Technologies (PETs) oplossingen voor privacy- en vertrouwenskwesaties. PETs bevatten verschillende technieken die ervoor zorgen dat er analyses kunnen worden gedaan op gegevens die zijn verhuuld. Deze technieken worden vaak gebaseerd op wiskundige algoritmen en cryptografische methoden. Gevoelige data worden hierbij zoveel mogelijk bij de bron gehouden. Enkel versleutelde data of gegevens die niet te herleiden zijn naar

een individu worden gedeeld en gebruikt voor een analyse, wat een breuk vormt met de traditionele methode waarbij data opgevraagd en centraal opgeslagen wordt.

Deze technologieën zijn voornamelijk relevant voor het verkrijgen van nieuwe inzichten op groepsniveau, bijvoorbeeld over de kwaliteit van geleverde zorg in Nederland, ongelijkheden in behandeling, gemiddelde levenskwaliteit en overleving bij hartfalen. Door onderzoek op groepsniveau kunnen ziektes beter worden voorspeld, wat de deur opent naar pro-actieve maatregelen. Als nodig kunnen

gegevens van individuen versleuteld aan elkaar gekoppeld worden, zodat bijvoorbeeld lange termijneffecten onderzocht kunnen worden. Kortom, deze technologische aanpak maakt het analyseren van gegevens uit verschillende bronnen mogelijk zonder gedetailleerde informatie te delen die gevoelige informatie van individuen onthult. Hierdoor worden zorgen, zoals schending van privacy en twijfels over de integriteit waarmee de andere partij de gegevens behandelt, weggenomen terwijl wel cruciale nieuwe inzichten kunnen worden verkregen.



In de cardiologie werken zorgpartners samen met TNO aan het Secur-e-Health-initiatief. Dit initiatief streeft naar verbeterd beheer van cardiovasculaire risico's, met name omdat maar liefst 80% van vroegtijdige hartziekten en beroertes te voorkomen is³. Het beoogt diepgaandere inzichten te verkrijgen in individuele verschillen, met inachtneming van de privacy van patiënten, zodat cardiovasculaire events eerder gesignaleerd kunnen worden. Daarbij wordt Federated Learning gebruikt, een technologie die te vergelijken is met een trein die langs verschillende stations rijdt, waarbij elk station staat voor een organisatie die data heeft van meerdere individuen⁴. De trein kan worden voorgesteld als een voorspellend model, dat steeds beter wordt naarmate het verder op weg is. Bij elk station leert het van de data ter plaatse, maar neemt deze niet mee. Zo blijft de privacy van de patiënten binnen elke organisatie gewaarborgd, terwijl het voorspellende model wordt verbeterd met behulp van diverse gegevensbronnen uit verschillende organisaties.

³ Cardiovascular diseases EURO (who.int)

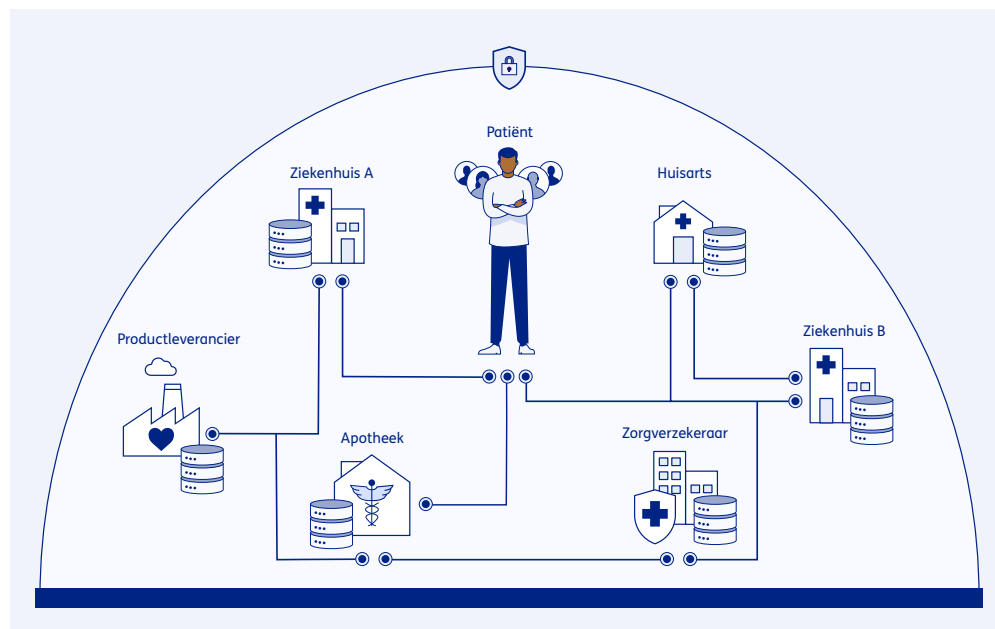
⁴ <https://pht.health-ri.nl/>

Data Spaces

Data Spaces concentreert zich op afspraken tussen verschillende partijen om data op een veilige en efficiënte manier te combineren, verrijken en analyseren. Organisaties hebben verschillende manieren van werken en gebruiken hun eigen, vertrouwde systemen. Zonder afspraken tussen partijen kan er geen veilige gegevensuitwisseling plaatsvinden. In overeenstemming met PETs benadrukt Data Spaces het belang van decentrale organisatie, in plaats van alle data op één centrale plek op te slaan. Door middel van een afsprakenstelsel wordt vastgelegd hoe gegevens worden gedeeld tussen organisaties, waarbij elke organisatie de controle over de eigen data behoudt. Deze integrale aanpak bevordert uniformiteit in werkwijzen, waardoor grootschalige implementatie mogelijk wordt binnen de gehele branche. Het streven is een Europese standaard voor onafhankelijk en gecontroleerd delen van gegevens, waarin het initiatief [International Data Spaces \(IDS\)](#) de leiding neemt.

Deze aanpak adresseert de zorgen van critici die lange tijd terughoudend

waren ten opzichte van initiatieven die trachten gegevens te centraliseren in grote centrale hubs of platforms. Hoewel samenwerken eenvoudig lijkt wanneer iedereen hetzelfde platform gebruikt, zoals Microsoft Teams, bestaan er naast beveiligingsrisico's en privacy bezwaren ook zorgen over afhankelijkheden van de platformaanbieder. Wat als een derde partij toegang krijgt tot het platform? Wat als het platform ineens vijfmaal duurder wordt? Een voordeel van Data Spaces is de flexibiliteit om met meerdere leveranciers te werken, voortkomend uit de erkenning van verschillende systemen en de noodzaak om zowel technische als governance obstakels te overwinnen. Deze benadering biedt een antwoord op de genoemde zorgen en bevordert daarmee vertrouwen in het delen en beheren van gegevens binnen de gezondheidszorg. In het kader van medisch onderzoek stimuleert gegevensverrijking diversiteit en nieuwe inzichten die verder gaan dan de traditionele focus op de witte man van 70 kilo, tussen de 20 en 40 jaar; de standaard proefpersoon die vaak gebruikt wordt in wetenschappelijk onderzoek⁵ en lange tijd de norm was in medisch onderzoek⁶.



In het samenwerkingsverband [HERACLES](#) bundelen dertien publieke en private partijen hun kennis om de impact van kanker te verminderen. Voor eierstokkanker worden recidieven in kaart gebracht; voor longkanker wordt ingezoomd op vroege signalering. HERACLES combineert Data Spaces en PETs om tegelijkertijd aan een technische infrastructuur die privacy waarborgt als aan een afsprakenstelsel te werken.

⁵ <https://www.ocw-verhalen.nl/verhalen/blinde-vlekken-in-de-wetenschap>

⁶ <https://fd.nl/tech-en-innovatie/1500341/de-ai-dokter-heeft-de-toekomst?gift=pM8lm>

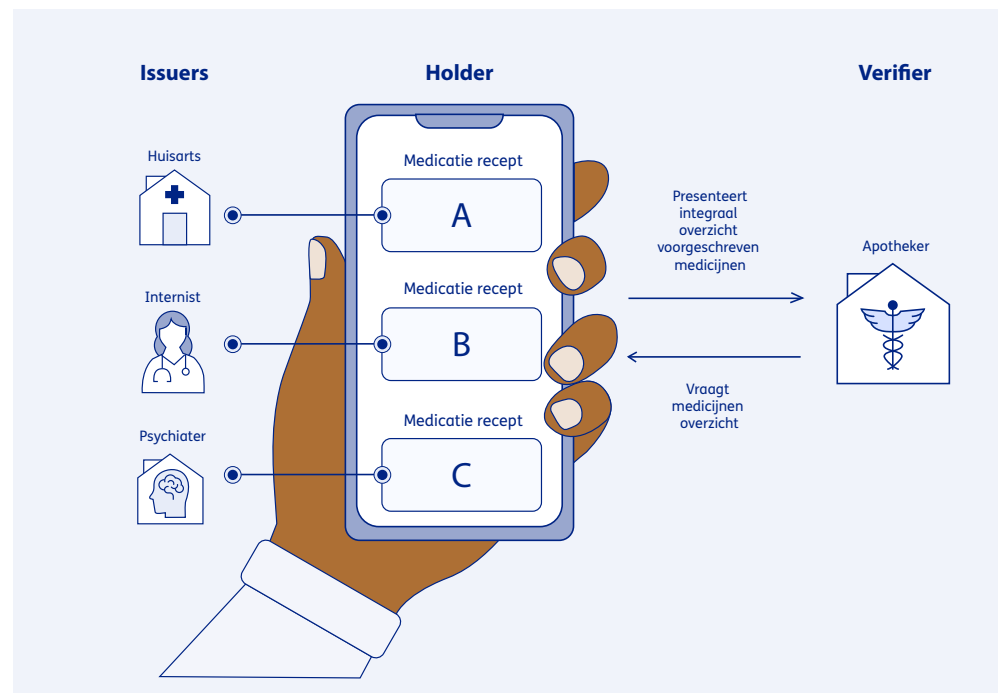
Self-Sovereign Identity

Self Sovereign Identity (SSI) is een onderzoeksveld dat zich richt op de systeemverandering die nodig is om vertrouwen in digitale gegevensuitwisseling te bevorderen. Daarnaast stelt het iedereen in staat om controle te hebben over welke informatie je met wie deelt. Met behulp van cryptografische methoden worden gegevens versleuteld, waarna precies kan worden gekozen welke informatie wordt gedeeld, passend bij het beoogde doel, zoals het aantonen van arbeidsongeschiktheid, zonder de aandoening bloot te geven. Daarnaast worden gegevens voorzien van digitale kenmerken, zoals een digitaal en onomstotelijk bewijs van BIG registratie, om de echtheid en geldigheid te verifiëren.

Door deze digitale gegevens op te slaan in een app op iemands telefoon, bijvoorbeeld die van een patiënt, krijgt die persoon controle. De patiënt kan nu zelf bepalen welke gezondheidsdata met wie worden gedeeld, zonder dat er iemand ongewenst kan meekijken. Daarnaast maakt deze benadering een integraal overzicht van een medisch dossier mogelijk: eenvoudig,

veilig en met waarborging van privacy, en onder controle van de patiënt. Zo kunnen patiënten altijd een actueel en verifieerbaar overzicht van hun medicatie bij zich dragen, dat te allen tijde voorgelegd kan worden aan een apotheek of een zorgverlener om contra-indicatie van nieuwe medicatie uit te sluiten. Kortom, SSI adresseert de frustratie over de overvloed aan gevoelige informatie die onnodig wordt gedeeld, het gebrek aan controle en het vertrouwen in de echtheid van gegevens. Het keert zich tegen de beweging waarin informatie zonder bewuste toestemming wordt verzameld en gebruikt voor doeleinden buiten het zicht van degene over wie het gaat. De gegevens behoren toe aan het individu, die zijn digitale identiteit moet kunnen beheren.

In de komende jaren zullen we door de introductie van de Europese Digitale Identiteit⁷ steeds meer mogelijkheden hebben om deze privacy preserving methode van gegevensuitwisseling te benutten. Ook nu al bestaan er al werkende implementaties: met Yivi kun je inloggen bij gemeentes⁸ of je KvK registratie inzien.⁹



Binnen het project Bio-Curify werken veertien partners afkomstig uit twee landen samen om de data, verkregen van slimme metingen in de thuissetting, in te zetten voor het behandelen van metaboolsyndroom. SSI zorgt voor meer controle over data, terwijl PET wordt ingezet om veilige analyses uit te voeren.

⁷ https://ec.europa.eu/commission/presscorner/detail/en/IP_23_5651

⁸ www.nijmegen.nl/diensten/privacy/yivi-nieuwe-manier-van-inloggen/

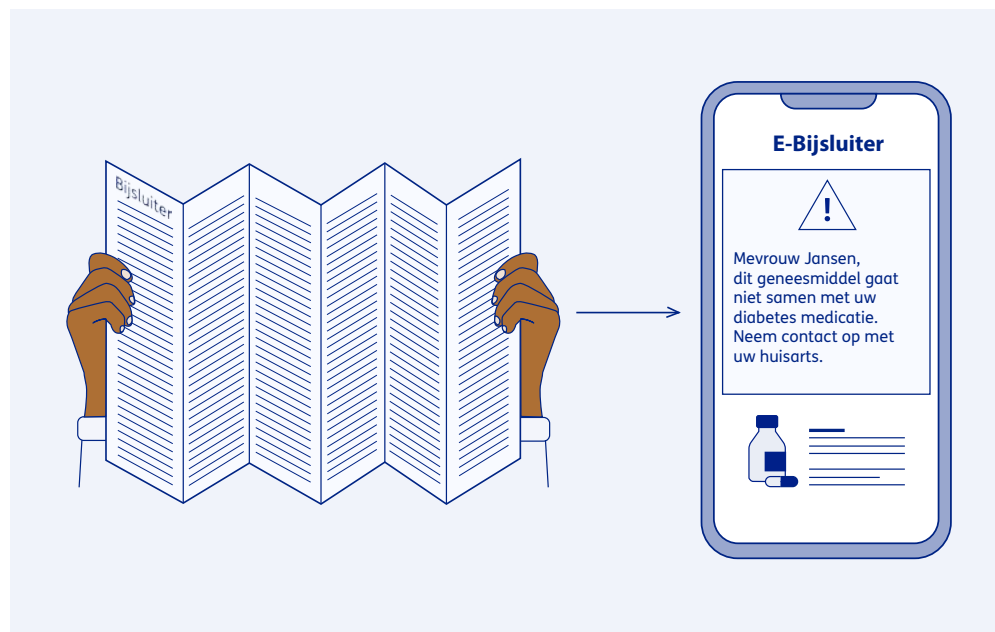
⁹ <https://www.yivi.app/voor-mij/meer-informatie-over-ophalen-gegevens-kamer-van-koop handelsregister>

Generatieve AI

Generatieve Artificial Intelligence (AI) richt zich op het genereren van nieuwe content, zoals tekst, afbeeldingen, audio of video gebaseerd op een grote hoeveelheid data. Door de snelle opkomst van taalmodellen, zoals ChatGPT, voeren computers al behoorlijk natuurlijke conversaties met gebruikers. ChatGPT is een bekend voorbeeld dat voornamelijk algemene informatie verstrekt, maar de ontwikkeling van gespecialiseerde chatbots maakt nauwkeurig advies op maat mogelijk. Daarnaast kan Generatieve AI communicatie met patiënten vereenvoudigen, toegankelijker maken, en een natuurlijker karakter geven, terwijl de administratieve last voor artsen afneemt. Voorbeelden zijn een arts die de computer gebruikt als sparringpartner voor diagnose, of een patiënt die een gepersonaliseerde uitleg krijgt over medicijngebruik, toegespitst op taal, complexiteit, en situatie. Een ander voorbeeld is het helpen van een patiënt bij het begrijpen van een ingewikkelde en lange bijsluiter.

Generatieve AI biedt oplossingen voor uitdagingen die gepaard gaan met de

grenzen van de menselijke capaciteit, zoals de gelimiteerde verwerkingscapaciteit van enorme hoeveelheden informatie. Er bestaat echter ook een schrikbeeld dat deze technologie huisartsen gaat vervangen en je als patiënt straks tegenover een robot komt te zitten. De medische chatrobot 'Med-Palm' beantwoordde een aantal medische vragen al bijna net zo goed als een echte arts. Recentelijk wist een computersysteem zelfs het Amerikaanse artsenexamen te halen¹⁰. Bij deze ontwikkelingen zijn er wel vragen over hoe actueel de informatie is, hoe betrouwbaar het advies, hoe reproduceerbaar de uitkomst en hoe de juridische verantwoordelijkheid geregeld is. Wie is er bijvoorbeeld aansprakelijk bij een verkeerd advies? Deze vragen worden binnen het onderzoeksveld van Generatieve AI aangepakt, bijvoorbeeld door het te combineren met eerdergenoemde doorbraaktechnologieën. Diverse partijen werken aan oplossingen die zowel patiënten als artsen ondersteunen, zonder inbreuk op privacy, afwijking van afspraken, verlies van datacontrole, en met een toetsbaar en transparant systeem.



TNO werkt mee aan GPT-NL, een eigen taalmodel in Nederland waar iedereen kan kijken hoe de achterliggende software werkt. Ook is te zien hoe de AI tot beslissingen komt¹¹ en wordt de privacy gewaarborgd in lijn met Europese waarden. Hierbij wordt een combinatie met de hierboven genoemde Privacy-Enhancing Technologies onderzocht. Ook is er aandacht voor aspecten als betrouwbaarheid en reproduceerbaarheid, en een correcte juridische inbedding.

¹⁰ 'Op weg naar de AI-dokter'. De Volkskrant 29 april 2023.

¹¹ [Nederland bouwt eigen open taalmodel GPT-NL - Digitale Overheid](#)

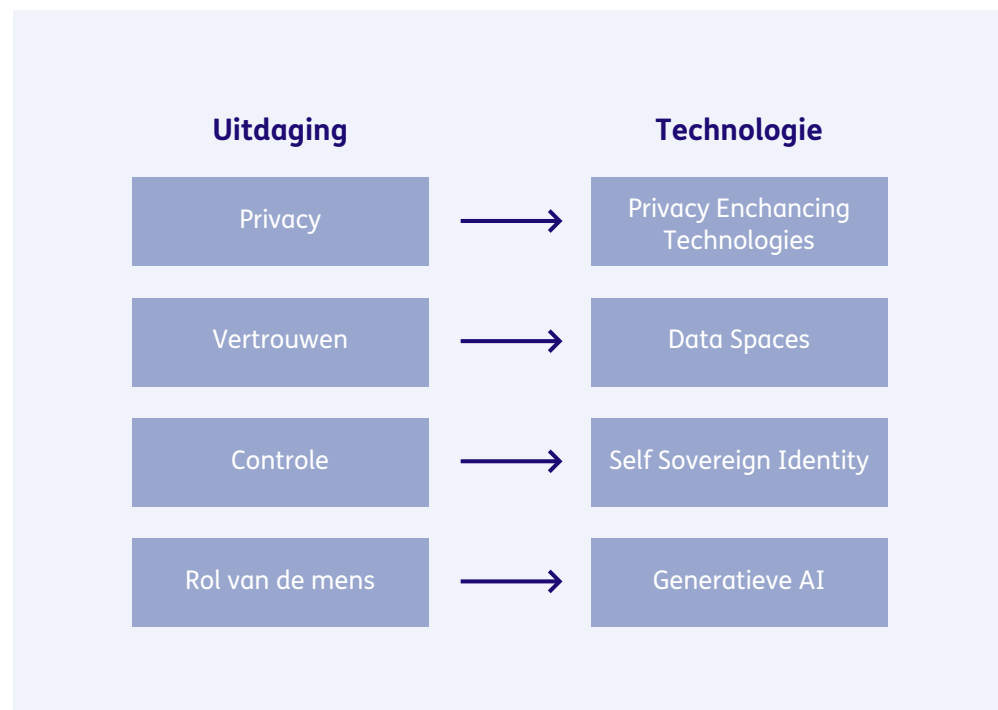
Conclusie

De datarevolutie in de zorg is even kansrijk als urgent. Dit is de tijd om de snelle ontwikkelingen in ons zorgsysteem in goede banen te leiden. We hebben de juiste technieken voor veilige, privacy-vriendelijke gegevensdeling en kunnen die op grote schaal toepassen. Privacy Enhancing Technologies waarborgen de privacy via innovatieve methodes. Data Spaces zorgt voor een branche brede en schaalbare oplossing die in de hele EU en daarbuiten resoneert. Self Sovereign Identity geeft de controle terug aan patiënten over hun eigen data. Als laatste maakt Generatieve AI het mogelijk om grote hoeveelheden informatie behapbaar te maken zonder de mens uit het oog te verliezen.

Met de nieuwe technologieën en het kader dat de EHDS biedt, kan ons zorgsysteem op alle fronten beter, betaalbaarder, bereikbaarder en persoonlijker worden. Dat biedt hoop en houvast in een tijd van vergrijzing en personeelstekorten, maar meer ook niet. Technologie en wetgeving mogen inmiddels gereed zijn, de zorgsector is dat nog niet. Om de beloofde grote stap voorwaarts te zetten, zullen grote én kleine spelers in de sector

zich snel moeten verdiepen in de gevolgen van de EHDS en de mogelijkheden van PETs, Data Spaces, SSI en generatieve AI. Vervolgens begint het echte werk: met nieuwe samenwerkingsverbanden, systemen en beleidskaders rondom het benutten van zorgdata. Technologie en systeemveranderingen gaan hand in hand. Dat die gaan komen is zeker. Hoe snel dat gebeurt en wie erover beslist niet. Er is een keuze. Wachten we af of nemen we met elkaar het initiatief. Het is daarbij van wezenlijk belang om het gesprek aan te gaan met andere partijen en gezamenlijk op te trekken. Succes maak je samen. Nodig experts uit voor concrete stappen en neem deel aan innovatieve projecten en pilots met andere (zorg)partijen om die in praktijk te brengen. Ga nu samen aan de slag, voor een duurzame toekomst van de gezondheidszorg.

TNO is de partij die op een onafhankelijke, betrouwbare en bovenal deskundige manier samen met welwillende partners het verschil kan maken op datagebied in zorg. Wil je weten wat de mogelijkheden zijn, neem contact met ons op.



Figuur 1. Veilig data uitwisselen. Let op: de technologieën bieden een oplossing voor meerdere uitdagingen. Ter illustratie benoemen we hierboven per technologie slechts één specifiek gebruiksscenario.

Auteurs

Sarah van Drumpt
Marie Beth van Egmond
Joachim de Greeff
Mike de Roode
Rik Rurup
Alexander van den Wall Bake
Jildau Bouwman
André Boorsma



Contact

Sarah van Drumpt

Researcher Cyber Security and Public Health

✉ Sarah.vandrumpt@tno.nl

☎ 0615421675

🌐 www.linkedin.com/in/sarahvandrumpt/

Alle rechten voorbehouden

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van TNO.

© januari 2024 TNO

