

Gebruik gezondheidsdata kan zonder privacyrisico's

Position paper TNO voor de rondetafel over beveiliging van patiëntengegevens van 27 maart 2025

Auteur ir F.W. (Freek) Bomhof

Inleiding

Voor het leveren en verbeteren van hoogstaande zorg is het meestal nodig om met data te werken. De beveiliging van deze data is van groot belang omdat het om gevoelige persoonsgegevens gaat: het is essentieel om onbevoegde toegang tot de data onmogelijk te maken. Vaak is de benodigde data op verschillende plaatsen aanwezig. Dit wordt dan vertaald naar de noodzaak om data te delen.

Het doel is niet om data te delen, het doel is om tot nieuwe inzichten te komen door te leren uit data.

Oproep aan de Tweede Kamer

1. Neem bij wetgeving over gevoelige data mee dat het mogelijk is om de risico's van informatielekkage vrijwel volledig te minimaliseren.
2. Wacht niet op meer onderzoek, privacy enhancing technologies zijn nu al in te zetten.
3. Dring aan op het gebruik van privacy enhancing technologies in de European Health Data Space.

Uitdagingen en oplossingsrichtingen

1: Neem bij wetgeving over gevoelige data mee dat het mogelijk is om de risico's van informatielekkage vrijwel volledig te minimaliseren

Uitdaging: Het delen van data vormt een risico. Dat geldt tijdens het delen (kopiëren en verplaatsen) ervan, maar ook als de data daarna op een extra plaats opgeslagen is. Om te voorkomen dat data tijdens het verplaatsen ervan onderschept kan worden, is het noodzakelijk uitsluitend niet-gevoelige (geaggregeerde) data te delen of deze te versleutelen. Om versleutelde data vervolgens te kunnen gebruiken moet deze weer ontsleuteld worden. Het risico is dan dat de data daarna toch op onbevoegde manier gebruikt wordt; hetzij door hackers, hetzij per ongeluk.

Oplossing: Een manier om deze risico's te minimaliseren wordt gevormd door een groep technologieën die ook wel 'Privacy Enhancing Technologies' (PET's) genoemd worden. Technologieën als *Multi-Party Computation* (MPC) en *Federated Learning* (FL) maken het mogelijk inzicht te verkrijgen door meerdere databronnen te koppelen, zonder daarbij in te boeten op privacy of vertrouwelijkheid. Er zijn overigens nog meer mogelijkheden: PET's vormen een gereedschapkast.

Met deze PET's kunnen analyses uitgevoerd worden op data die met verschillende wiskundige technieken onherkenbaar gemaakt is. De onderliggende data hoeven dus niet in leesbare vorm te worden gedeeld om analyses uit te voeren en nieuwe inzichten te verkrijgen. Resultaat is dat er geen gevoelige informatie naar andere partijen 'lekt' en er alléén bewerkingen mogelijk zijn die tot het vooraf overeengekomen eindresultaat leiden.

Het is dus meestal niet nodig om data in leesbare vorm te delen. Privacy Enhancing Technologies geven invulling aan het principe 'houd data bij de bron' (dit is ook het leidende principe achter de [Inter-Bestuurlijke Data Strategie](#) van de overheid). Belangrijk is wel: Privacy Enhancing Technologies zijn geen manier om de AVG te omzeilen. De data wordt echt verwerkt dus er blijft een rechtsgrond nodig. PET's zorgen ervoor dat dataminimalisatie, doelbinding en proportionaliteit maximaal worden ingevuld.

In haar '[Sectorbeeld Overheid](#)' constateert de Autoriteit Persoonsgegevens dat bestuurders te weinig kennis hebben van PET's. *Ze worden nog veel te weinig gebruikt.*

Een voorbeeld is de opzet van Transactie Monitoring Nederland (TMNL), met als doel het tegengaan van witwassen: dit werd teveel als een niet-proportioneel 'sleepnet' gezien en de aanpak is verlaten. Een oplossing op basis van PET's zonder zo'n centrale database is echter goed mogelijk, zeker nu er een nieuwe Anti Money Laundering Regulation van kracht is.

In een recente sessie begeleidingsethiek over het combineren van data uit de JGZ-wereld en CBS, werd geconstateerd dat er behoefte is aan data-standaardisatie in een sterk gefragmenteerd veld, behoefte aan data-soevereiniteit, en behoefte aan samen optrekken als community waarbij alle partijen analyses kunnen doen in plaats van alleen onderzoeksinstanties die analyses kunnen doen.

2: Wacht niet op meer onderzoek, PET's zijn nu al in te zetten

Uitdaging: Implementatie van PET's leidt tot handelingsverlegenheid bij bestuurders. Privacy wordt beschouwd als een 'gevaarlijk' onderwerp. Het 'tijd kopen' door een extra onderzoek uit te laten voeren lijkt dan een aantrekkelijke optie.

Oplossing: Verschillende bedrijven, zowel in Nederland als daarbuiten, leveren deze technologie al operationeel. Belangrijkste belemmeringen zijn nog de onbekendheid met deze mogelijkheden, terughoudendheid bij privacy officers, en technologische puzzels in de informatiehuishouding.

Inmiddels zijn er al verschillende toepassingen van deze aanpak operationeel. Zo wordt de internationale samenwerking tussen Financial Intelligence Units met volledig behoud van privacy ondersteund, kan met behoud van proportionaliteit vastgesteld worden welke Nederlanders mogelijk recht hebben op de Aanvullende Inkomensvoorziening Ouderen, of kunnen organisaties cyberincidenten melden aan het NCSC op volledig anonieme wijze. Ook kleinere organisaties passen ze toe.

In het gezondheidszorgdomein zijn er diverse toepassingen, bijvoorbeeld bij het Integraal Kankercentrum Nederland, dat samen met zorgverzekeraars en farmaceuten een datasamenwerking rond zorgdata (van o.a. ziekenhuizen en huisartsen) heeft opgezet om specifieke aspecten van longkanker en eierstokkanker beter te begrijpen. *Deze toepassing moeten echter worden verbreed.*

3: Dring aan op het gebruik van PET's in de European Health Data Space

Uitdaging: Met de invoering van de European Health Data Space (EHDS) wordt het delen en hergebruiken van gezondheidsdata in Europa niet alleen aangemoedigd, maar ook gereguleerd met bindende verplichtingen voor lidstaten. Dit creëert grote kansen voor innovatie en betere zorg, maar brengt tegelijkertijd serieuze uitdagingen op het gebied van privacy en databescherming met zich mee.

Oplossing: Om te voldoen aan de EHDS-verplichtingen én de privacy van burgers te waarborgen, zijn PET's essentieel. De uitwerking van de EHDS in Nederland vindt nu plaats door de Health Data Access Body NL (betrokken zijn ICTU, CBS, RIVM en Health-RI) en de ontwerpkeuzes voor de komende jaren worden nu gemaakt. Bij deze uitwerking zou naast de klassiekere, meer gecentraliseerde aanpak ook het gebruik van PET's veel explicieter moeten worden meegenomen: PET's kun je namelijk niet makkelijk later toevoegen, we moeten ze nu in het ontwerp opnemen.

Contactpersoon: Tim Kreuk, Manager Public Affairs (tim.kreuk@tno.nl)