ESSAY

NAAR EEN PERSOONLIJK GEZONDHEIDS DOSSIER DAT WERKT

Consumenten eHealth ontwikkelt zich razend snel. En Nederland is niet klaar voor verantwoord beheer en uitwisseling van de data die daaruit voort gaan komen. Urgente vraag: houden we de consumentendata in eigen hand of laten we ze aan de commercie over?

tekst **Neeltje Vermunt en Theo Hooghiemstra**

IN ZIJN PAS VERSCHENEN ADVIES CONSUMENTEN-EHEALTH BRENGT DE Raad voor de Volksgezondheid en Zorg[1] de opkomst van consumenten-eHealth onder de aandacht. De focus van dit essay ligt op een onderdeel van dat advies: het verwerken[2] van persoonsgegevens[3], in het bijzonder gezondheidsgegevens[4]. Onder consumenten eHealth verstaat de Raad zonder tussenkomst van zorgverleners aan de consument aangeboden informatie- en communicatietechnologie, die beoogt de gezondheid van gebruikers te ondersteunen of te verbeteren.

VERDIENMODELLEN

In het huidige zorgsysteem speelt consumenten-eHealth nog geen significante rol. De ontwikkelingen zullen elkaar echter snel opvolgen en consumenten-eHealth kan de reguliere zorg op verschillende manieren ingrijpend gaan veranderen. Het gaat namelijk niet alleen om toepassingen voor wellness en lifestyle, maar toenemend ook om toepassingen voor zelfdiagnostiek en zelfbehandeling. Consumenten-eHealth haakt direct in op wensen van mensen en biedt hen gevraagde en ongevraagde mogelijkheden. Gebruikers krijgen hiermee de kans om de zorg voor hun gezondheid zo veel mogelijk zelf vorm te geven. De Raad verwacht een gedeeltelijke vervlechting van consumenten-eHealth en reguliere zorg. Op onderdelen zou consumenten-eHealth reguliere zorg zelfs kunnen vervangen. De randvoorwaarden voor gegevensverwerking zijn momenteel echter nog onvoldoende ingesteld op de opkomst van consumenten-eHealth en de veranderingen in de zorg die daaruit voort kunnen vloeien. Dit is een urgent probleem, want de ontwikkelingen gaan door. Wanneer geen adequate voorwaarden worden geschapen, zullen normen, kaders, faciliteiten en procedures door de verschillende commerciële leveranciers (van consumenten-eHealth) en hun verdienmodellen worden bepaald. Dit zou het benutten van de mogelijkheden van consumenten-eHealth voor mens en maatschappij sterk kunnen beperken.
Op dit moment worden gegevens die door betrokken zorgverleners (en de persoon zelf) worden verzameld nauwelijks onderling uitgewisseld. Bescherming van privacy is een belangrijk aandachtspunt. Absolute bescherming van privacy, in de zin van volledig controle hebben over de eigen informatie, is onmogelijk te realiseren. Privacy moet gezien worden in een bepaalde context. Een specifiek aandachtspunt op het gebied van privacy is de koppeling van gegevens uit consumenten-eHealth en de reguliere zorg bij verdergaande vervlechting.
Belangrijk probleem daarbij is dat gezondheidsgegevens gegenereerd buiten het zorgdomein niet worden beschermd door het beroepsgeheim van de WGBO. Zonder beroepsgeheim kunnen bijvoorbeeld politie, justitie en inlichtingendiensten zoals de National Security Agency (NSA) gegevens vorderen.

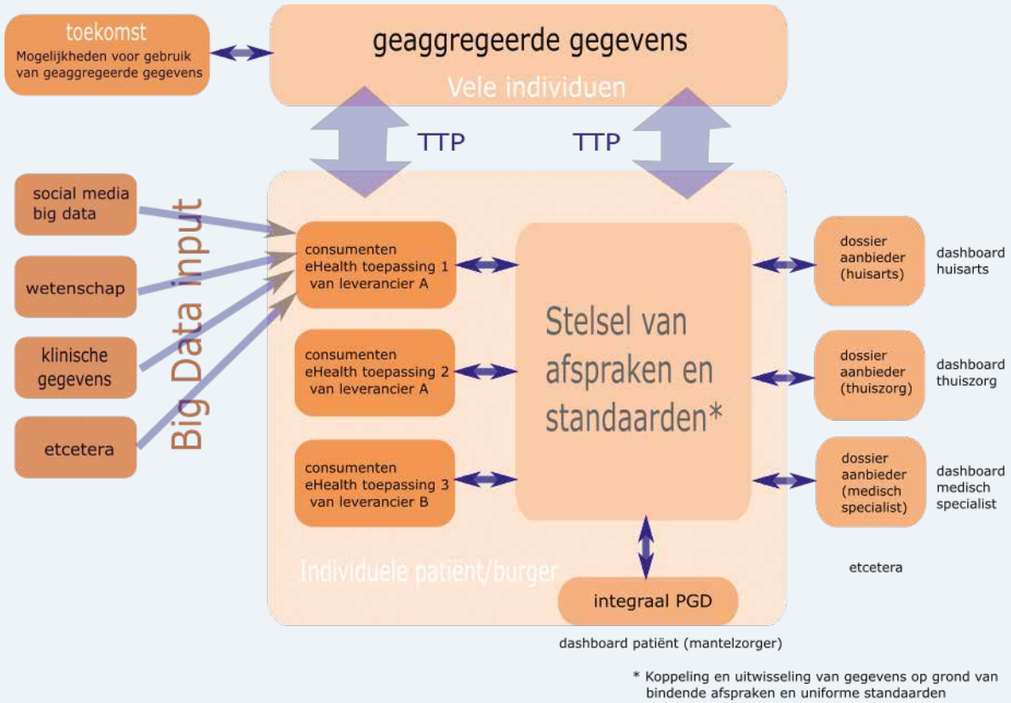
Bescherming van privacy is ook van belang op geaggregeerd niveau. Consumenten-eHealth genereert grote hoeveelheden gegevens. Op geaggregeerd niveau kunnen deze gegevens worden gekoppeld met gegevens uit andere bronnen en waardevolle informatie opleveren. Deze informatie kan heel waardevol zijn voor bijvoorbeeld wetenschappelijk onderzoek. Misbruik is echter ook mogelijk, bijvoorbeeld door profiling en monitoring.
Ook is de vraag voor wie de big data (op geaggregeerd niveau) in geanonimiseerde vorm toegankelijk zullen zijn en wie beschikking en zeggenschap krijgt over de resultaten van mogelijke analyses op deze big data. Een belangrijk onderdeel van het businessmodel van sommige bedrijven die gezondheidsplatforms aanbieden, kan bestaan uit inkomsten uit de verkoop van informatie verkregen uit big data. Mensen zijn zich er vaak niet van bewust dat hun gegevens verkocht kunnen worden. Afnemers kunnen kapitaalkrachtige bedrijven zijn. In dit geval hebben publieke instanties en onderzoeksinstellingen zoals universiteiten mogelijk veel minder toegang tot deze informatie. Hierdoor kan de wetenschap op achterstand geraken en zouden publieke taken duurder kunnen worden.
Een ander belangrijk probleem bij verwerking van persoonsgegevens zijn gebrek aan standaardisatie, interoperabiliteit en dataportabiliteit met het bijbehorend risico van een *vendor-lock-in*. De RVZ heeft over dit probleem geadviseerd in zijn *Advies Patiënteninformatie* (2014).
Tenslotte vormt een gebrek aan betrouwbare authenticatiemiddelen een reëel gevaar. Betrouwbare authenticatiemiddelen zijn een voorwaarde voor zeggenschap door consumenten/patiënten via digitale inzage en toegang tot gegevens en bieden bescherming tegen identiteitsfraude. Op dit moment is er nog geen gratis, nationaal bruikbaar en voldoende betrouwbaar authenticatiemiddel voor consumenten-eHealth en dat is een belangrijk probleem bij verdere verspreiding.

PERSOONLIJK GEZONDHEIDS DOSSIER

Om gebruik te kunnen maken van gegevens vanuit verschillende bronnen met zeggenschap bij de desbetreffende persoon zelf, zijn voorwaarden nodig, juist ook op het gebied van elektronische gegevensverwerking.
In zijn advies visualiseert de raad een mogelijk toekomstig neutraal stelsel van bindende afspraken en uniforme informatiestandaarden om te voorzien in adequate voorwaarden voor gegevensverwerking.
Vertrekpunt in deze figuur (zie figuur p.62) is een persoon. Deze persoon kan zelf gegevens verzamelen via verschillende apps (aan de linkerzijde). Behalve door de desbetreffende persoon worden gegevens verzameld door andere betrokkenen, veelal zorgverleners zoals een huisarts, een medisch specialist, de thuiszorg, maatschappelijk werk en zo verder. Gegevens die verzameld worden door alle betrokkenen kunnen toegankelijk gemaakt worden door koppeling en uitwisseling op grond van het te ontwikkelen stelsel van afspraken en standaarden. Toepassingen moeten aansluiten bij deze afspraken en uniforme standaarden.
Met toestemming van de desbetreffende persoon kunnen relevante gegevens uit de verschillende dossiers geautomatiseerd opgevraagd, gekoppeld en samengebracht toegankelijk gemaakt worden via een relevant dashboard. Een persoonlijk gezondheidsdossier[5] kan fungeren als dashboard voor de burger. Dit PGD voor en door mensen geeft de mens een centrale rol in de zorg voor zijn of haar gezondheid en welbevinden. Hierdoor kunnen toepassingen steeds beter aansluiten bij en geïntegreerd worden in iemands dagelijks leven. De consument kan een keuze maken uit verschillende PGD's en krijgt de mogelijkheid om met behoud van gegevens over te stappen naar een andere aanbieder van een PGD.
In zijn advies doet de RVZ de aanbeveling aan de overheid om de opzet van een dergelijk stelsel te stimuleren. Hierin zou aansluiting gezocht kunnen worden bij internationale standaarden. Zeggenschap van de consument/patiënt is een van de uitgangspunten. Bescherming van zijn

1 De Raad voor de Volksgezondheid en Zorg (RVZ) en de Raad voor Maatschappelijke Ontwikkeling (RMO) zijn per 1 januari 2015 samengevoegd tot de Raad voor Volksgezondheid en Samenleving (RV&S).
2 In navolging van de Wet bescherming persoonsgegevens (Wbp) verstaan we onder verwerken: alles wat met persoonsgegevens kan worden gedaan van verzamelen tot vernietigen.
3 Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 1 Wbp).
4 Gezondheidsgegevens: alle persoonsgegevens die de lichamelijke of geestelijke gesteldheid betreffen (artikel 21 Wbp).

DE VOORGESTELDE GEGEVENSVERWERKING GEVISUALISEERD.



gegevens wordt gerealiseerd door *privacy by design*. Gegevens van verschillende consumenten-eHealth-toepassingen en door zorgverleners gegenereerde gegevens moeten zonder problemen gekoppeld kunnen worden. Gegevens moeten kosteloos en zonder tussenkomst van derden door consumenten zelf bij een andere aanbieder ondergebracht kunnen worden. Software-updates moeten geborgd zijn. Bij de opzet van dit stelsel van afspraken en standaarden zal ook het aspect van toezicht en handhaving betrokken moeten worden.

ZELFDIAGNOSE

Breed gedragen, vertrouwde en veilige gegevensverwerking vergt hoogwaardige authenticatie en ingebouwde autorisatie. Betrouwbare authenticatiemethoden zijn een voorwaarde voor zeggenschap van zorgconsumenten via digitale inzage en toegang tot gegevens. Daarnaast bieden ze bescherming tegen identiteitsfraude. Bruikbare methoden voor authenticatie zouden met voorrang ontwikkeld moeten worden.

Ook het patiëntengeheim[6] is van belang, voor zover het medisch beroepsgeheim geen bescherming biedt om burgers te beschermen tegen het opvragen van vertrouwelijke gezondheidsinformatie door derden.

Een van de apps die personen zullen kunnen gebruiken, is een app voor zelfdiagnose/zelfbehandeling, die onder andere door middel van big data-analyse uit verschillende bronnen zelfdiagnostiek en behandeling mogelijk maakt. Een van de bronnen wordt gevormd door geaggregeerde en geanonimiseerde gezondheidsgegevens van vele individuen. Deze gegevens kunnen met toestemming van de desbetreffende personen en waarborgen door een Trusted Third Party[7] (TTP) op vertrouwde en veilige wijze toegankelijk gemaakt worden voor de app, zonder dat deze direct tot de persoon herleidbaar zijn. Op deze manier kunnen algoritmen steeds verder verbeterd worden. Naast op het desbetreffende individu toegespitst advies in diagnostiek en behandeling, ontstaan ook nieuwe mogelijkheden voor wetenschap en beleid door analyse van instant *feedback loops* en *machine learning* op grond van geaggregeerde en geanonimiseerde gezondheidsgegevens met waarborgen door een TTP.

Zo kunnen inherente en instant mogelijkheden voor kwaliteitsborging, performance management van zorgverleners en automatische declaraties ontstaan. Zowel (individuele) prestaties in de zin van toegevoegde waarde aan ‘gezondheid en welbevinden’ als ‘verantwoord handelen’ kunnen inzichtelijk worden gemaakt. Bekostiging op basis van uitkomsten wordt mogelijk. Gegevens worden het nieuwe ‘zwarte goud’.

CONCLUSIE

De ontwikkelingen op het gebied van consumenten-eHealth gaan snel. De RVZ adviseert daarom de minister om de opzet van een neutraal stelsel van bindende afspraken en uniforme standaarden voor gegevensuitwisseling te stimuleren. Daarnaast beveelt de RVZ aan om te zorgen voor betrouwbare authenticatiemiddelen als voorwaarde voor zeggenschap van consumenten/patiënten over de toegang tot hun gegevens en als bescherming tegen identiteitsfraude. ◆

Neeltje Vermunt is werkzaam bij de RV&S als senior adviseur en verantwoordelijk voor het project ‘Consumenten eHealth’. Theo **Hooghiemstra** is algemeen secretaris/directeur van wat tegenwoordig de Raad voor Volksgezondheid & Samenleving (RV&S) heet.

5 verdere informatie zie het RVZ-advies Patiënteninformatie (RVZ, 2014)
6 Voor verdere informatie zie het RVZ-advies Patiënteninformatie (RVZ, 2014)