Privacy by Design & MedMij

MedMij
Grip op je eigen gezondheidsgegevens

Gegevensdeling in zorg
PI.Lab en ECP bij HagaZiekenhuis

22 februari 2017, Marcel Heldoorn en Theo Hooghiemstra

Opzet

I. Wat en waarom (Afsprakenstelsel) MedMij?
II. Breed begrip privacy
III. Wbp en AVG in een notendop
IV. Privacy by Design
V. Privacy by Design en MedMij
VI. Privacy-juridisch kader MedMij
VII. Overige juridische aspecten MedMij

vanderSar
@Patient2punt0

Volgen

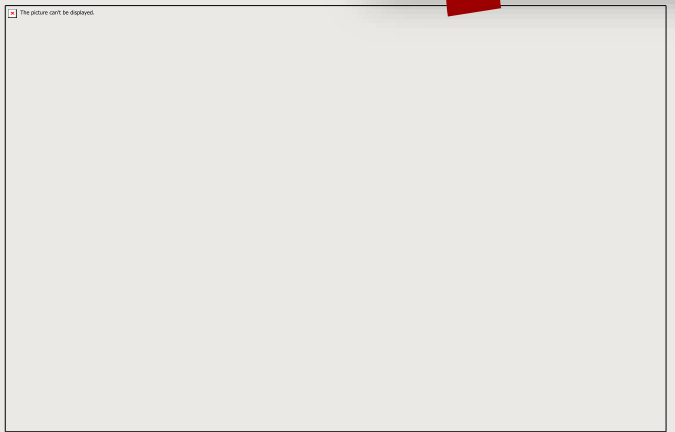
Heb es bedacht waar m'n medische gegevens zijn: 3 ziekenhuizen (8 afd.), 2 huisartsen, 4 fysiotherapeuten, revacentrum #EPD #PHR @NPCF

Beantwoorden Retweeten Toevoegen aan favorieten

2 augustus 12 om 1:03 's ochtends via web · Deze tweet embedden

2013


Het persoonlijk gezondheidsdossier
De visie van patiëntenfederatie NPCF
PERSOONLIJK GEZONDHEIDS-DOSSIER


The picture can't be displayed.

juli 2014 RVZ rapport Patiënteninformatie

4 juli 2014 | Dit persbericht hoort bij het advies Patiënteninformatie

Geef patiënt de beschikking over al zijn gezondheidsinformatie in een PGD

De patiënt moet, het liefst met één druk op de knop op een website, inzicht krijgen in zijn/haar medische dossier. Patiënten moeten uiteindelijk zelf hun persoonlijk gezondheidsdossier (PGD) kunnen beheren. Om de privacy te waarborgen voor de patiënt dient er een 'patiëntgeheim' te komen, in aanvulling op het medisch beroepsgeheim voor zorgprofessionals. Ook is het noodzakelijk om bij de inrichting van het PGD de privacynormen in te bouwen *(privacy bij design)*.
Om kwaliteit, toegankelijkheid en betaalbaarheid van de zorg te verbeteren is het verder noodzakelijk dat niet-identificeerbare gezondheidsinformatie beschikbaar komt voor publieke doeleinden.
Voor deze veranderingen is het nodig dat het ministerie van VWS de regie neemt om te zorgen dat relevante partijen in de zorg bindende besluiten nemen over de inrichting van de informatievoorziening in de zorg. Dat staat in het advies 'Patiënteninformatie, informatievoorziening rondom de patiënt' dat de Raad voor de Volksgezondheid en Zorg (RVZ) vandaag aanbiedt aan Leon van Halder, SG van

Contactpersoon

Mr. drs. T.F.M. (Theo) Hooghiemstra

Publicaties

Patiënteninformatie
(pdf – 1MB)

Nieuwsbrief RVZ

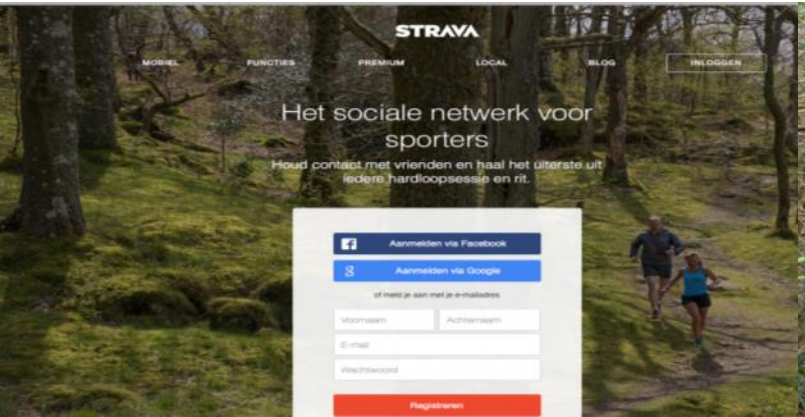
De RVZ verstuurt regelmatig een nieuwsbrief per e-mail. U kunt zich hier gratis op abonneren.

Naam

E-mailadres

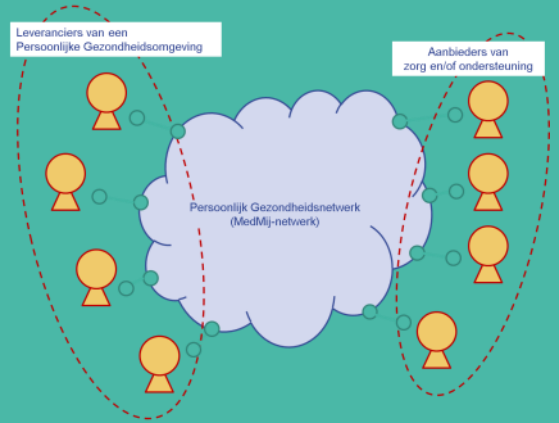
Hoe het nu gaat.

- Steeds meer mensen willen aan de slag met hun gezondheid
- En houden vaker zelf informatie over hun gezondheid bij
- Groei van aanbod patiëntportalen
- Voor patiënten zijn gegevens zijn versnipperd en niet overal toegankelijk
- Zorgverleners weten niet wat de patiënt doet
  (wat slikt de patiënt?)



Informatieberaad

Samen werken aan een duurzaam informatiestelsel voor de zorg



- Ideaal: In 2020 kan **iedereen** die dat wil **online** zijn eigen **gezondheidsgegevens verzamelen en gebruiken**. Veilig en uit allerlei bronnen. Dit geeft mensen **meer grip op hun eigen gezondheid**.

- **Afsprakenstelsel** met juridische, organisatorische, financiële, semantische en technische afspraken

- **Partijen die deelnemen** aan het afsprakenstelsel **committeren zich aan de afspraken** en kunnen via het netwerk hun diensten aanbieden

Wat doet MedMij?

- Randvoorwaarden voor opschaling van persoonlijke gezondheidsomgevingen:
  - Informatiestandaarden voor gegevensuitwisseling
  - Afsprakenstelsel voor vertrouwen
  - Scenario's voor financiering

- Belangrijk:

  we maken géén persoonlijke gezondheidsomgeving!

MedMij

Grip op je eigen gezondheidsgegevens

MedMij ontwikkelde in 2016:

- Standaarden voor medicatie, labuitslagen, allergieën en zelfmetingen.
- Basiseisen voor persoonlijke gezondheidsomgevingen en ICT-systemen.
- Afsprakenstelsel voor MedMij-deelnemers.
- Inzicht in kosten en baten van het gebruik van persoonlijke gezondheidsomgevingen.

Wat doen we in 2017?

MedMij
Grip op je eigen gezondheidsgegevens

Toetsen

- Met onze partners toetsen we de MedMij-standaarden, basiseisen en afspraken in de praktijk.
- Daarin wisselen zorgaanbieders gezondheidsgegevens uit met persoonlijke gezondheidsomgevingen van patiënten;
- en andersom.

Wat doen we in 2017?

MedMij
Grip op je eigen gezondheidsgegevens

Verbreden

- We versnellen de ontwikkeling van nieuwe MedMij-standaarden.
- We gaan van 4 soorten informatie naar meer dan 20 voor diverse sectoren van zorg en gezondheid.
- We sluiten aan bij sectorplannen, programma's en initiatieven in de omgeving van MedMij.

Wat doen we in 2017?

MedMij
Grip op je eigen gezondheidsgegevens

Verbeteren

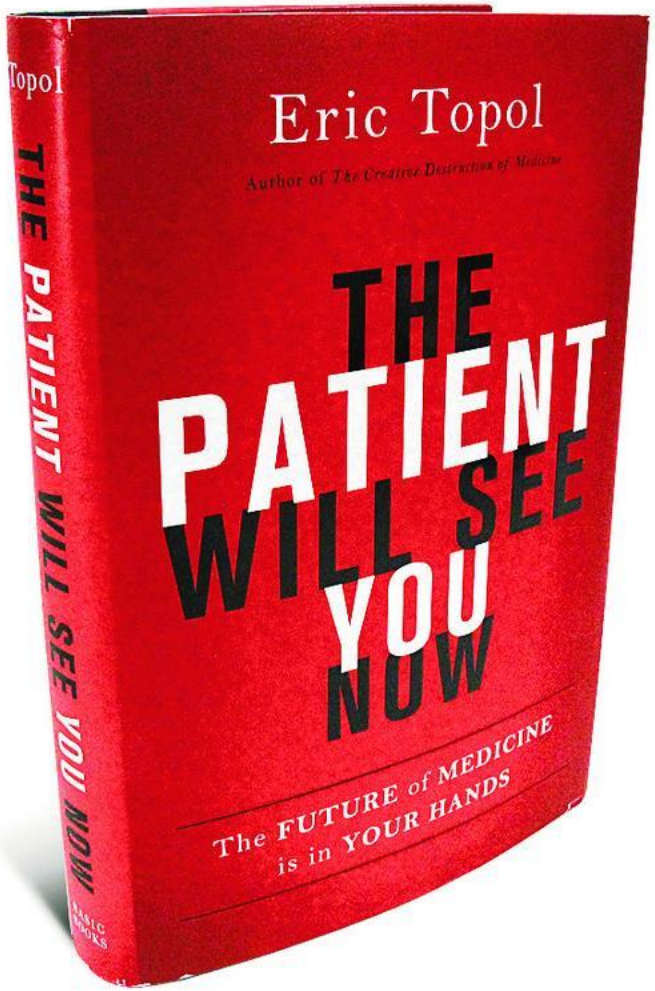
- We evalueren continu met de ervaring van leveranciers, zorgaanbieders en patiënten.
- En maken businessmodellen die het gebruik van persoonlijke gezondheidsomgevingen stimuleren.

I. Afbakening

- **Gegevensuitwisseling in netwerk via provider tussen PGO-en en systemen** van **zorgaanbieders** en **overheden**.
- MedMij **richt zich (nog) niet** op:
  - **Keurmerk** persoonlijke gezondheidsomgevingen (functionaliteiten);
- MedMij **richt zich wel** op :
  - **Voorwaarden** voor **aansluiting** op het **stelsel**
- **Planning**: april versie 0.1. en Open Marktconsultatie.
- **PGO bijv**: Meddex, Zorgkluis, Patient1, Quli, Philips, Apple, Microsoft.
- **Relaties** o.a. QIY (TrustFramework); DTLS (FAIR/healthtrain).
- **FAIR-principes** (Findable, Accessible, Interoperable, Reusable).
- **Vervolg presentatie**: Privacy by Design: juridisch-organisatorisch.

II. Breed Privacy-begrip

- Niet absoluut, niet vloeibaar. Grondrecht/ Menselijke waardigheid
- Bescherming persoonsgegevens én informationele zelfbeschikking
- Bescherming persoonsgegevens: Wbp/meldplicht datalekken/AVG
- Technische én organisatorische maatregelen
- Informationele zelfbeschikking (inzage, regie, biografie leven)
- Strenge (privacy)wetgeving: continue innovatie! Vb: milieu


Topol
THE PATIENT WILL SEE YOU NOW
Eric Topol
Author of The Creative Destruction of Medicine
THE PATIENT WILL SEE YOU NOW
The FUTURE of MEDICINE is in YOUR HANDS

III. Wbp en AVG in een notendop

- Wbp: transparantie, doelbinding (noodzaak!)), beveiliging, dataminimalisatie en rechten van betrokkenen (inzage, correctie, verwijdering)
- AVG = Wbp +

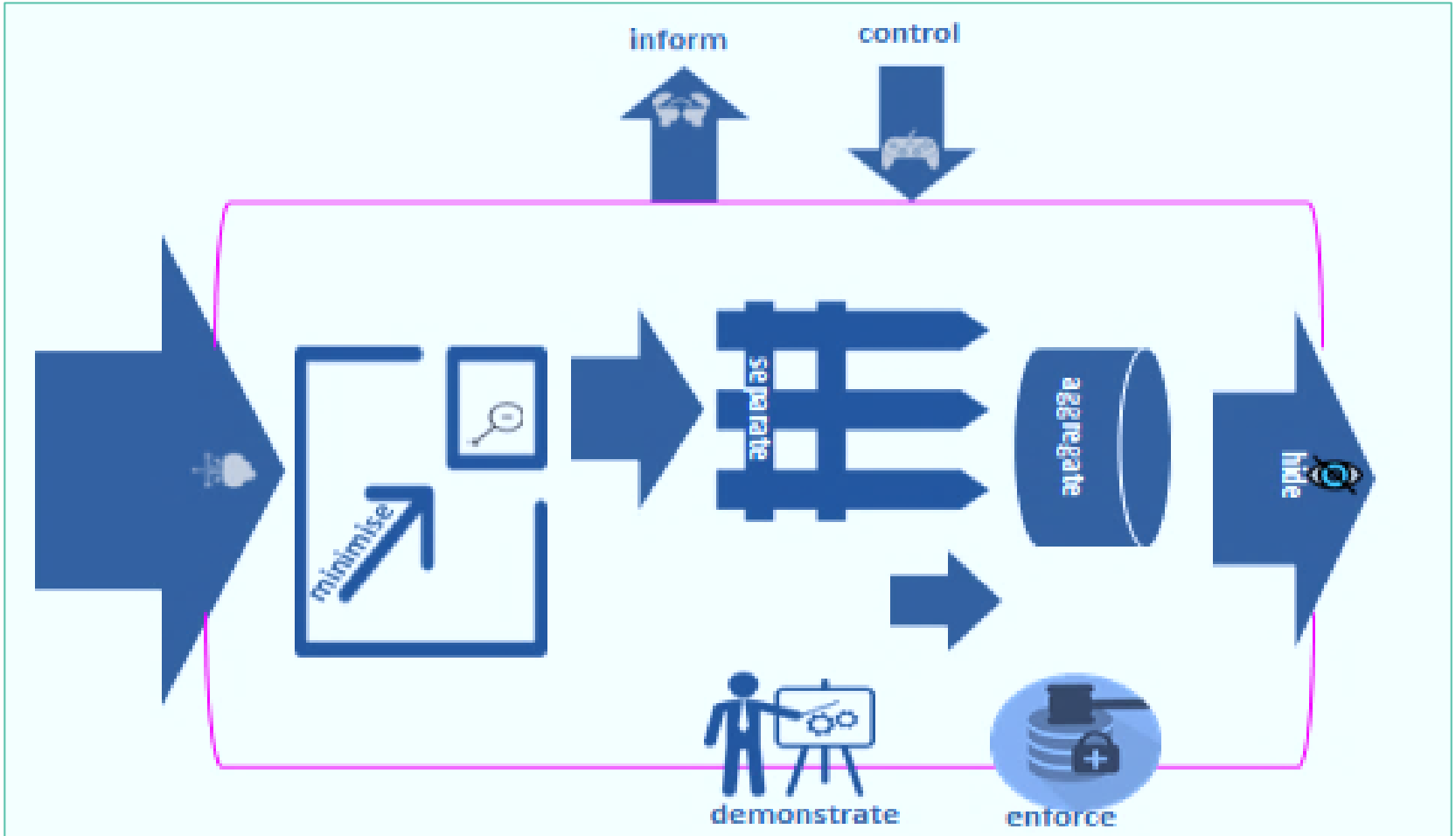
1) Accountability (documenteren, implementeren, transparantie t/m algoritmes);
2) Extra rechten: vergeetrecht, dataportabiliteit,
3) Privacy by design! (Wbp kende al dataminimalisatie en PET)
4) Privacy Impact Assessment
5) Hoge boetes
6) strenger voor bewerkers / verwerkers (mede-aansprakelijk)
7) Bepaling over profileren (artikel 22 AVG)

IV. Privacy by design

- Vanuit het brede privacy-begrip: combinatie van technische en organisatorische maatregelen (incl. afspraken en governance) waar privacybeginselen niet technisch zijn af te dwingen worden afgedwongen.

- Focus deze presentatie: afsprakenstelsel MedMij,vooral op de organisatorische maatregelen. In de andere presentaties wellicht meer nadruk op de technische maatregelen. Beide noodzakelijk!

- Privacy vanaf de eerste ontwerpstappen meenemen bij keuzes.


inform
control
minimise
separate
aggregate
hide
demonstrate
enforce

V. Privacy by Design & Afsprakenstelsel MedMij

- Gegevensbescherming door ontwerp en door standaardinstellingen
- Privacy Gap Assessment uitgevoerd
- Privacy belangrijk aandachtspunt in het gehele ontwikkelproces
- Afsprakenstelsel start kleinschalig
- Afspraken in afsprakenstelsel voor providers binnen netwerk vertalen in aansluitvoorwaarden PGO-leveranciers en zorgaanbieders.

VI. Privacy-juridisch kader

- **Verantwoordelijke**: partij die alleen, of samen met anderen het doel en middelen voor de verwerking vaststelt. Gelden plichten wet voor.
- **Persoon is geen verantwoordelijke**! (anders geen enkele partij met plichten jegens hem en heeft persoon geen rechten. Hij kan niet echt doel/middelen bepalen, geen echte macht, geen maatwerk p.p.), PGO-leveranciers en zorgaanbieders wel.
- **Zeggenschap in plaats van eigendom op persoonsgegevens**!
- **Bewerker**. In AVG verwerker, met aansprakelijkheid. Mogelijke afspraak: provider alleen als bewerker: slechts in opdracht van verantwoordelijke handelen. Niet gegevens voor eigen doeleinden.

VI. Privacy-juridisch kader

- **Gezondheidsgegevens en BSN:** bijzondere gegevens.
- **Nee, tenzij** wettelijke grondslag. **BSN vergt wet**, gezondheidsgegevens **wet of toestemming. Geen MedMij-wet**: grondslag toestemming. **Toestemming garantie**? Vrijwillig? Onder druk grote bedrijven of overheden: Zoiets als **patiëntgeheim** nodig? Andere waarborgen?
- **Proportionaliteit en subsidiariteit: dataminimalisatie**!
- **Patiëntauthenticatie**: Gezondheidsgegevens + BSN + (medisch) beroepsgeheim): eIDAS: substantieel of hoog. Rapport PrivacyCare en PBLQ. Strategie: groeipad!

VI. Privacy-juridisch kader

- **Passende beveiligingsmaatregelen**: minimaal aansluiten bij ISO/NEN-normen. Inclusief vertrouwensketen: identificatie, authenticatie, autorisatie en logging + versleuteling. End-to-end encryptie vereist voor partijen in MedMij-netwerk, beveiligde mail, datalekken melden.
- **Gedrag en bewustwording**, naast providers, PGO-leveranciers en zorgaanbieders ook personen (gebruikersvoorwaarden)
- **Governance en privacyorganisatie**: beheerorganisatie (toe- en uittredingseisen providers) met privacy-aanspreekpunt, periodieke audits, maatregelen niet nakomen afspraken, crisis (DigiNotar)
- **Vrije, uitdrukkelijke en specifieke toestemming** voor verwerken gezondheidsgegevens, wettelijke grondslag voor BSN.

VI. Privacy-juridisch kader

- **Doelbinding**: doel MedMij is inzage en regie persoon over eigen gezondheidsgegevens. Mag persoon alles verwerken in PGO?
- **Profilering**: is een ander doel, mag dat? In ieder geval beperkt door artikel 22 AVG, toestemming en geen besluiten met rechtsgevolg.
- **Kwaliteit**: informatie van persoon, zorgaanbieders, al dan niet erkend? Wearables? Kwaliteit van de data? Via logging /timestamps bijhouden.
- **Gegevensverwerking buiten EU?** Landen moeten vallen onder Privacy Shield / adequaatheidsbesluit. Daarbuiten (te) riskant.
- Standaard-(model)- **bewerkersovereenkomst**, bijv. met providers?
- **Geheimhoudingsbepalingen** voor degenen met toegangsrechten.

VI. Privacy-juridisch kader

- **Zorgaanbieders** (Wgbo: medisch beroepsgeheim, recht niet weten,vernietigingsrecht bewaartermijn 15 jaar of langer, wet BSN in de zorg, Wet aanvullende bepalingen verwerking persoonsgegevens zorg, straks Wet generieke diensten infrastructuur)
- **Personen met PGO buiten zorgaanbieder**: geen wettelijke bescherming geheimhouding, risico's profilering, bewaartermijn levenslang?, wellicht geen BSN (pseudoniemen?), ook de andere wetten niet, wel: Wbp/AVG en de providers ook telecomwetgeving.
- **PGO bij zorgaanbieder:** kan dat? Landelijk? Wel beroepsgeheim/BSN?
- **Waarborgen en afspraken over continuïteit, datalekken, incidenten, calamiteiten- en crisisplan** (bijv. leren van DigiNotar).
- **Vernietiging**: recht om vergeten te worden…..

VI. Privacy-juridisch kader

- **Transparantie**: kenbaar maken aan persoon welke gegevens en desgevraagd ook algoritmes. Accountability, incl. toestemming.
- **Persoon heeft recht op**: inzicht gegevens die verantwoordelijke verwerkt, recht op inzicht derde landen, vergetelheid (toestemming intrekken, lukt het om bij alle partijen te verwijderen? Afspraken nodig! Bij zorgaanbieders: vernietigingsrecht), dataportabiliteit (standaardisatie!).

VII. Overige juridische aspecten

- Noodzaak van een **Wet op persoonlijke gezondheidsomgevingen”?**
  Zaken regelen die niet in afsprakenstelsel kunnen zoals:
  - “**Persoonlijke gezondheidsomgeving-geheim**”
  - **Toezicht en handhaving**
- **Aansprakelijkheid** van zorgaanbieders, PGO-leveranciers en providers.
- Mogelijk ook aansprakelijkheid persoon?
- **Vertegenwoordiging**
- **Gezondheidsapps**: app met gezondheidsgegeven een **medisch hulpmiddel**?
- …..