aan	Tweede Kamer - commissie VWS
cc	Tweede Kamer - commissie DiZa
ons kenmerk	SPF20260511
datum	11 mei 2026
onderwerp	Inbreng Privacy First CD digitalisering 21 mei 2026

Geacht Kamerlid,

In het commissiedebat *'digitale ontwikkelingen in de zorg'* gaat u van diverse kanten gewezen worden op het belang van 'databeschikbaarheid'. Dat belang onderschrijven wij volledig.

Aan de wijze waarop dit zou moeten gaan gebeuren, het **grootschalig** en **ongericht** delen van medische gegevens, kleven echter enorme risico's voor de privacy en digitale veiligheid van patiënten.

Over het antwoord op de vraag *"waarom?"* is brede consensus. Voor de autonomie van burgers, zeggenschap van patiënten en ons vertrouwen in de zorg is de vraag *"hoe?"* nu essentieel.

Onderstaande analyse helpt bij het stellen van precies die vraag.

Met vriendelijke groet,

Marc Smits
Beleidsadviseur Stichting Privacy First
marc@privacyfirst.nl
06-52471179

Inleiding

De spreekkamer van de dokter moet een veilige plek zijn voor iedere patiënt. Je dokter belooft je alles geheim te houden, dus kan je daar in goed vertrouwen alles bespreken. Deze belofte, het medisch beroepsgeheim, is een cruciaal fundament van ons vertrouwen in onze zorgverleners en de zorg als geheel.

Maar dit fundament is aan het verdwijnen. Doordat medische gegevens **grootschalig** en **ongericht** beschikbaar worden gesteld, kan de dokter de belofte van geheimhouding niet meer waarmaken. De arts heeft namelijk geen zicht meer op wie daadwerkelijk toegang heeft tot patiëntgegevens.

Dat kan ook anders. Bij het **gericht** beschikbaar stellen van gegevens (binnen het zorgproces) houden patiënt en arts samen de regie op wie toegang heeft. Dat regelen ze onderling in de spreekkamer: eenvoudig, laagdrempelig, efficiënt en met de beste privacybescherming.

Recente hacks en geopolitieke ontwikkelingen laten zien dat de risico's van grootschaligheid en het 'platformdenken' niet alleen in theorie bestaan. Daarmee is het van groot belang dat uw Kamer zich *nu* buigt over **hoe** data beschikbaar wordt gesteld in de zorg.

De regie hoort thuis bij patiënten en hun zorgverleners. Hun autonomie dient verankerd te zijn en te blijven in het ontwerp van de digitale infrastructuur.

Gericht beschikbaar

Het **gericht beschikbaar** stellen van gegevens werkt tussen zorgverleners onderling. De set van gegevens is beperkt tot wat voor deze behandeling relevant is en wordt gedeeld met één, of een beperkte groep zorgverleners. Bijvoorbeeld: een doorverwijzing naar een afdeling in het ziekenhuis, of verstrekken van een recept.

Deze methode is de eenvoudigste, veiligste en veruit de goedkoopste vorm van databeschikbaarheid. Het sluit naadloos aan op het beroepsgeheim en biedt daarmee de beste privacybescherming. Als patiënt heb je geen digitale portals, apps of voorzieningen nodig. Je regelt het in de spreekkamer, samen met je zorgverlener.

Gerichte beschikbaarheid werkt met name (maar niet uitsluitend) bij een planbare patiëntreis.

Ongericht beschikbaar

Bij het **ongericht beschikbaar** stellen van gegevens wordt een verzameling van patiëntgegevens breed raadpleegbaar gemaakt voor grote groepen zorgverleners, zonder dat op voorhand bekend is voor wie precies.

De ongerichte methode is in elke situatie toepasbaar, maar vereist een complexe, grootschalige implementatie. Patiënten moeten op voorhand toestemming geven, dus ook als ze überhaupt nog geen patiënt zijn. Dat wordt al snel bijzonder ingewikkeld, met als gevolg dat patiënten te grote sets gegevens delen met duizenden zorgverleners tegelijk.

Infrastructuur

Om gegevens op te kunnen vragen moet je weten waar je ze kan vinden. Er is dus een lijst nodig van alle patiënten en hun behandelaren (lokalisatie). Daarna moet ‘ergens’ worden bepaald welke gegevens door wie *mogen* worden opgevraagd (autorisatie), op basis van de eerder gegeven toestemming.

Deze combinatie van grootschalige gecentraliseerde voorzieningen zorgt voor enorme risico’s voor de privacy & digitale veiligheid en torenhoge kosten. De beheerders ervan bepalen, onder invloed van een politiek krachtenveld, welke keuzevrijheid patiënten overhouden. Hackers krijgen een one-stop-shop voor toegang tot alles, van iedereen.

Politieke realiteit

Toch is de beleidslijn van het Ministerie van VWS om, samen met partijen in het zorgveld, **alle** medische gegevens van **iedereen** grootschalig **ongericht** beschikbaar te stellen[1]. De zorgverzekeraars, ziekenhuizen, zorgkoepels en de Patiëntenfederatie zijn gezamenlijk verantwoordelijk voor de ontwikkeling van centrale onderdelen in de technische infrastructuur, waaronder de online toestemmingsvoorziening 'Mitz'. Het platform 'Cumuluz' moet patiëntgegevens gaan delen, maar gaat draaien op het Amerikaanse Microsoft Azure.

De mogelijkheid gegevens **gericht** beschikbaar te stellen lijkt nauwelijks in beeld bij de zorgkoepels. Die hebben zich al jaren geleden (na de afwijzing van de wet-EPD) gecommitteerd aan het gedachtegoed van **ongerichte** beschikbaarheid van gegevens, vanuit het idee dat ze zo invloed zouden hebben op de koers.

Conclusie

Het **gericht beschikbaar** stellen van gegevens is toepasbaar in veruit de meeste situaties. Er is geen grootschalige, complexe technologie nodig, die dus ook niet grootschalig gehackt kan worden. Een vergrijzende groep patiënten wordt niet opgezadeld met het gebruik van technologische voorzieningen die ze niet nodig hebben.

Met **gerichte beschikbaarheid** blijft de regie, de sturingsmacht, bij de twee stakeholders waar het werkelijk om draait: de patiënt & zorgverlener(s). Andere stakeholders, de veldpartijen en het Ministerie, leveren dan echter sturingsmacht in. Daar ligt de politieke uitdaging.

Onze oproep aan uw Kamer: besluit dat **gerichte databeschikbaarheid** overal in de zorg technisch gerealiseerd moet worden.

---

[1] Brief van de Minister van VWS, 27529, nr. 326, 18-12-2024
https://www.tweedekamer.nl/downloads/document?id=2024D50947

Kamervragen

- Kan de Minister aangeven op welke wijze zij ervoor gaat zorgen dat gerichte databeschikbaarheid (dus tussen zorgverleners onderling) straks overal in de zorg mogelijk is?
- Kan de Minister aangeven op welke wijze ze gaat zorgen voor een open en transparante *governance* voor databeschikbaarheid en zorgcommunicatie, waardoor bijvoorbeeld ook burgerrechtenorganisaties kunnen deelnemen.

Ontwikkeling Mythos doet NSC'er Gotink denken aan de ontdekking van buskruit

Van Sparrentak somt op: „Mythos opent de deur naar grootschalige cyberaanvallen. Denk aan gehackte banken, ontregelde transportsystemen en ziekenhuizen zonder stroom". Ze vervolgt: „Mythos is slechts het eerste model. En met een Amerikaanse overheid die niet gelooft in het reguleren van AI, zijn we overgeleverd aan [de welwillendheid van] techbedrijven."

Bron: NRC, vrijdag 8 mei 2026, pagina 23