Bijlage

De Nederlandse zorg digitaliseert in hoog tempo. Daarbij wordt steeds sterker ingezet op centrale infrastructuren voor gegevensuitwisseling en toestemmingsregistratie, zoals het Landelijk Schakelpunt (LSP), Mitz en toekomstige Europese systemen onder de European Health Data Space (EHDS).

Hoewel deze systemen worden gepresenteerd als efficiënt en noodzakelijk voor databeschikbaarheid, brengen zij ook aanzienlijke risico's met zich mee. Centrale systemen vergroten de impact van hacks, datalekken en ongewenste toegang tot medische gegevens. Wanneer toegang tot grote hoeveelheden patiëntinformatie afhankelijk wordt van centrale infrastructuren, ontstaat een aantrekkelijk doelwit voor cybercriminaliteit.

Stichting Decozo pleit daarom voor blijvende ruimte voor decentrale alternatieven voor gegevensuitwisseling. Het gaat om systemen waarbij gegevens gericht worden gedeeld tussen direct betrokken zorgverleners, onder regie van arts en patiënt, zonder brede beschikbaarstelling via centrale infrastructuren.

Push autorisatie is een voorbeeld van zo'n decentrale standaard. Deze vorm van gegevensuitwisseling sluit aan bij bestaande wetgeving en bij meerdere moties en amendementen die door beide Kamers zijn aangenomen sinds de afwijzing van het landelijke EPD[1].

Het probleem van centrale gegevensuitwisseling

De huidige ontwikkeling in de zorgdigitalisering beweegt zich richting steeds grotere en centraler georganiseerde systemen voor gegevensuitwisseling, zoals het Landelijk Dekkend Netwerk (LDN) en de EHDS. Daarbij blijft de medische informatie zelf vaak opgeslagen bij de zorgverlener, maar wordt de toegang tot die gegevens geregeld via centrale infrastructuren en toestemmingssystemen.

---

[1] 2011:Motie-Tan Y inz. wettelijke eisen elektronische patiëntendossiers, EK 31 466 W
2014: Motie-Leijten, geen financiële stimulans deelname LSP, EK 33 509 nr. 34
2016: Motie-Bredenoord inz. databescherming by design EK 33 509 R
2016: Motie-Teunissen EK inz. decentraal toegankelijk houden van dossiers,33 509 T
2018: Motie- Van Kooten-Arissen/Hijink inz. realisatie decentrale koppelvlakken 29 515 nr. 425
2019: Motie van Kooten-Arissen/Hijink LSP geen verplichte infrastructuur, 27.529 nr. 174
2019:Motie van Kooten-Arissen/Hijink inz. end-to-end beveiliging 27 529 nr. 176
2023: Motie Gerkens c.s., inz. decentrale infrastructurele voorzieningen EK 35 824 I

Voorbeelden hiervan zijn het Landelijk Schakelpunt (LSP), Mitz en centrale voorzieningen binnen het Landelijk Dekkend Netwerk (LDN) en de EHDS. Zo speelt binnen het LDN de centrale toestemmingsvoorziening Mitz een spilfunctie als centrale arbiter die beslist wie bij bepaalde gegevens mag.

Deze ontwikkeling vergroot de impact van beveiligingsincidenten. Wanneer toegang tot medische gegevens afhankelijk wordt van centrale systemen, kunnen inbreuken in die systemen verstrekkende gevolgen hebben voor grote groepen patiënten tegelijk.

Recente incidenten laten zien dat ook grote professionele organisaties kwetsbaar zijn voor cyberaanvallen. Denk aan de hack bij ChipSoft, maar ook aan eerdere incidenten bij Clinical Diagnostics, Odido en internationale zorgpartijen zoals UnitedHealth. Het risico bestaat dat met een grotere verbondenheid van zorgsystemen en uitwisselingssystemen - én de toegenomen dreiging van hacks door AI - de impact van hacks zoals die bij ChipSoft nog vele malen groter wordt.

Het risico zit niet alleen in het stelen van gegevens uit één systeem, maar steeds vaker ook in het misbruiken van gehackte systemen om elders medische gegevens op te vragen. Hoe groter en centraler de infrastructuur, hoe groter de potentiële impact van een succesvolle aanval.

Daarnaast dreigt in de praktijk een situatie te ontstaan waarin patiënten nauwelijks nog een reële keuze hebben om buiten dergelijke systemen te blijven. Dat schuurt met het uitgangspunt van vrijwillige toestemming en met het medisch beroepsgeheim.

Waarom decentrale alternatieven nodig zijn

Stichting Decozo pleit niet tegen digitale gegevensuitwisseling, maar vóór **gerichte** gegevensuitwisseling onder directe regie van patiënt en zorgverlener.

Bij (zuiver[2]) decentrale gegevensuitwisseling wordt vooraf duidelijk welke zorgverlener toegang krijgt tot welke gegevens. Alleen direct betrokken zorgverleners krijgen toegang, zonder dat dossiers ook breed beschikbaar worden gesteld aan andere zorgverleners.

Dit heeft belangrijke voordelen:

- minder afhankelijkheid van centrale systemen;
- een kleiner aanvalsvlak voor hackers;
- meer regie voor patiënt en zorgverlener;

---

[2] Soms worden systemen decentraal genoemd terwijl alleen de data decentraal opgeslagen en beheerd wordt - maar bijvoorbeeld toegangscontrole gecentraliseerd is via een landelijke voorziening. Wij bedoelen met decentraal systemen waarbij zowel de regie decentraal (bij arts en patiënt) ligt én de technologie zo veel mogelijk decentraal is geïmplementeerd. Zie https://decozo.org/uitgangspunten-voor-decentrale-standaarden

- meer flexibiliteit binnen het zorgproces;
- betere bescherming van het medisch beroepsgeheim.

In de praktijk verloopt een groot deel van de zorg al via gerichte communicatie tussen bekende zorgverleners, bijvoorbeeld bij verwijzingen, overdrachten of medicatieprocessen. Decentrale communicatie sluit beter aan op deze praktijk dan systemen die uitgaan van brede databeschikbaarheid.

Centrale en decentrale infrastructuren hoeven elkaar daarbij niet uit te sluiten. Net als in het verkeer kunnen verschillende vormen van infrastructuur naast elkaar bestaan voor verschillende doelen. Centrale systemen kunnen nuttig zijn voor bepaalde toepassingen, maar mogen niet de enige optie worden.

Push autorisatie als decentrale standaard

Push autorisatie is een communicatiemodel voor gerichte en decentrale gegevensuitwisseling zonder centrale toegangssystemen[3].

Bij push autorisatie wisselen direct betrokken zorgverleners gegevens uit via beveiligde autorisaties vanuit de bronhouder. Alleen specifiek geautoriseerde zorgverleners kunnen gegevens ophalen. Tijdens transport worden gegevens end-to-end beveiligd uitgewisseld.

Het systeem ondersteunt daarmee gegevensuitwisseling binnen het bestaande zorgproces, zonder brede beschikbaarstelling van medische dossiers.

Doordat het systeem geen centrale componenten bevat, zijn alleen specifieke partijen - de zorgverleners die toegang krijgen - in staat om gegevens op te halen. Dit maakt het ‘aanvalsvlak’ voor hackers veel kleiner dan bij centrale systemen die gegevens breed beschikbaar stellen.

Push autorisatie is reeds toegepast binnen de huisartsenzorg en wordt momenteel meegenomen in verschillende proof-of-concepts[4] en pilots rond gegevensuitwisseling, onder andere met apothekers. De ervaringen laten zien dat gerichte en veilige gegevensuitwisseling technisch goed mogelijk is zonder afhankelijkheid van centrale infrastructuren[5].

---

[3] https://decozo.org/standaarden/

[4] Aanbesteding PoC/pilots voor de implementatie van generieke functies voor gegevensuitwisseling, ministerie van VWS, 2026. Zie https://decozo.org/nieuws .

[5] https://whiteboxsystems.nl/pilot-resultaten https://decozo.org/nieuws

Wetgeving en keuzevrijheid

Sinds de afwijzing van het landelijke EPD in 2011 heeft het parlement meermaals uitgesproken dat gegevensuitwisseling in de zorg niet uitsluitend afhankelijk mag worden van centrale systemen.

Push autorisatie sluit aan bij diverse moties en amendementen die sinds 2011 door beide Kamers zijn aangenomen. Daarnaast sluit het aan bij artikel 14 lid d van de Wegiz, waarin is vastgelegd dat verplichte gegevensuitwisseling nooit uitsluitend via een Elektronisch Uitwisselingssysteem (EUS) mag plaatsvinden[6].

Deze waarborg is van groot belang. In de praktijk dreigt namelijk een situatie te ontstaan waarin patiënten feitelijk geen alternatief meer hebben voor deelname aan centrale infrastructuren zoals het LSP, Mitz of toekomstige Europese systemen onder de EHDS.

Wanneer deelname aan dergelijke systemen noodzakelijk en dus impliciet vereist wordt voor goede zorg, komt vrijwillige toestemming onder druk te staan. Daarmee ontstaat spanning met fundamentele uitgangspunten uit de AVG en het medisch beroepsgeheim.

Decentrale alternatieven zijn daarom niet alleen technisch relevant, maar ook van belang voor keuzevrijheid, proportionaliteit en vertrouwen in de zorg.

Conclusie

Decentrale systemen voor gegevensuitwisseling bieden patiënten en zorgverleners meer regie, flexibiliteit en bescherming tegen de risico's van grootschalige centralisatie.

Stichting Decozo pleit daarom voor een gezondheidsinformatiestelsel (GIS) waarin decentrale. gerichte gegevensuitwisseling structureel naast centrale systemen voor databeschikbaarheid blijft bestaan.Dat vraagt om:

- blijvende ruimte en middelen voor decentrale standaarden;
- bescherming van artikel 14 lid d van de Wegiz;
- ondersteuning van gerichte gegevensuitwisseling binnen het zorgproces;
- en blijvende keuzevrijheid voor patiënten en zorgverleners.

Alleen zo kan digitale gegevensuitwisseling in de zorg veilig, proportioneel en toekomstbestendig worden ingericht.

Een goed afgewogen mix van centrale en decentrale systemen maakt het systeem veiliger en robuuster tegen hacks en disruptie van (centrale) systemen, en het biedt gegevensuitwisseling in de zorg ook flexibiliteit doordat binnen het zorgproces gemakkelijker maatwerk kan worden

---

[6] De standaard sluit ook aan bij de NEN normen die in het kader van de Wegiz ontwikkeld worden, zie https://www.nen-egiz.nl .

toegepast bij het uitwisselen van gegevens. Ook voorkomt het problemen die samenhangen met marktdominantie en data soevereiniteit.

Over stichting Decozo

Decozo is in 2022 opgericht met als missie om decentrale gegevensuitwisseling breed geïmplementeerd te krijgen in Nederland en daarbuiten. In de visie van Decozo moeten arts en patiënt binnen het eigen zorgproces de volledige regie houden over de uitwisseling van gegevens. Externe partijen of systemen die kwetsbaarheden introduceren en die niet strikt noodzakelijk zijn, worden uit de architectuur geweerd..

Decozo beheert technische specificaties (standaarden) van decentrale communicatie-systemen via een not-for-profit model, door deze specificaties beschikbaar te stellen aan leveranciers die deze willen implementeren. Concreet betreft dit heden de standaarden voor *push autorisatie.*

Het governance model van Decozo is zo ingericht dat privacy van patiënten blijvend beschermd kan worden terwijl standaarden zich doorontwikkelen. We doen dit door privacy organisaties duurzaam te betrekken bij het goedkeuringsproces voor de technische documentatie en specificaties.