Technische ontwikkelingen rondom databeschikbaarheid in de zorg

versie: 14 april 2025

Eigen keuzes
in een vrije omgeving

Stichting Privacy First
Nieuwe Herengracht 49
1011 RN Amsterdam

https://privacyfirst.nl
info@privacyfirst.nl
+31 20 810 0279

KVK 34298157
ANBI erkend

Inleiding

Wij zien een infrastructuur ontstaan met systeemrisico's die vele malen groter zijn dan het Landelijk EPD uit 2011. De belangrijkste oorzaak hiervoor is de wijze waarop de governance in de zorg georganiseerd is en de vervlechting van belangen van betrokken partijen.

De technische infrastructuur moet ruimte bieden voor inclusiviteit. Dat vereist een open en transparante governance, zodat (onder andere) ook de belangen van privacy en burgerrechten vertegenwoordigd kunnen worden.

Onderstaand volgt een analyse vanuit technisch perspectief, met de nadruk op normen voor autorisatie en lokalisatie van gegevens. Belangrijkste doel hiervan is om te laten zien dat alternatieve concepten en oplossingen mogelijk zijn die wel voldoen aan de eis van subsidiariteit.

Generieke functies (NEN)

Bij het uitwisselen van medische gegevens zijn er een aantal processen die altijd plaatsvinden, ongeacht de wijze en inhoud van de uitwisseling. Dit zijn 'generieke functies' en hiervoor worden, in het kader van de Wegiz[1], standaarden ontwikkeld binnen de NEN. Het doel is om systemen in de zorg op dezelfde wijze te laten functioneren en communiceren, waardoor 'interoperabiliteit' ontstaat.

Op dit moment onderscheiden we de volgende generieke functies.

Identificatie & authenticatie

Wie ben je en kan je dat bewijzen?

Een zorgverlener is een natuurlijk persoon met een BIG-registratie, werkzaam voor een zorginstelling. Je paspoort is je identificatiemiddel. Het CIBG verstrekt een verklaring van inschrijving in het BIG register en de zorginstelling verklaart dat de persoon bij de instelling werkt. Deze 'attributen' zijn digitale bewijsmiddelen, nodig voor het opvragen van gegevens.

Toestemming

Met wie wil je gegevens delen?

Bij een doorverwijzing spreekt het eigenlijk voor zich dat relevante gegevens worden verstrekt aan de volgende zorgverlener. Een zorgverlener mag dan 'veronderstellen' dat een patiënt hiermee instemt: 'veronderstelde toestemming'.

In andere situaties is een 'uitdrukkelijke toestemming' van de burger/patiënt vereist, bijvoorbeeld voor deelname aan een Elektronisch UitwisselingsSysteem[2] (EUS) en het op voorhand ongericht delen van gegevens.

Lokalisatie

Welke patiëntgegevens bevinden zich waar?

Bij een doorverwijzing is het duidelijk dat de gegevens zich bevinden bij de doorverwijzende zorgverlener. Wil je een meer volledig overzicht van alle (historische) gegevens, dan zal je een lijst (index) bij moeten houden. Zorgverleners zullen de gegevens die ze opslaan moeten registreren bij een index. Dit kan een landelijke of regionale (centrale) index zijn maar dit is niet altijd nodig. Er bestaan verschillende oplossingen voor het opslaan, zoeken en versturen van lokalisatie informatie (zie aparte bijlage).

---

[1] Wet elektronische gegevensuitwisseling in de zorg

[2] Artikel 15a Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)

Autorisatie

Wie mag welke gegevens inzien?

Op basis van een wettelijke grondslag, zoals toestemming, kan er aan de zorgverlener een 'toegangsbewijs' worden verstrekt waarmee deze een bepaalde set (lokalisatie) gegevens kan opvragen. Bij een doorverwijzing kan dit toegangsbewijs direct worden meegestuurd.

Bij het opvragen van gegevens uit een index zijn er afspraken nodig waarin wordt vastgelegd welke zorgverleners, onder welke condities gegevens mogen opvragen. Deze afspraken komen uiteindelijk terecht in een 'matrix', een tabel met (bijvoorbeeld) de 'rolcodes' van zorgverleners en specificatie van gegevens waar zorgverleners met deze rol toegang toe mogen hebben.

Adressering

Van instellingen (en afdelingen binnen instellingen)

Net als in onze papieren wereld heeft een zorginstelling een digitaal adres nodig en een doorverwijzing gaat 't.a.v. afdeling X'. Voor deze generieke functie is identificatie en authenticatie noodzakelijk. Voor adressering is nog geen normontwikkeling gestart bij de NEN.

Implementatie door VWS en koepels (IZA)

Het Ministerie en stakeholders uit het IZA implementeren nu 'generieke voorzieningen' voor de generieke functies. Deze zijn gecentraliseerd en voldoen daarmee slechts gedeeltelijk aan de 'generieke functies' die zijn beschreven in de NEN normen.

Identificatie & authenticatie

(eIDAS-2 & Wet DIAZ, voor nu buiten beschouwing gelaten)

Toestemming

Voor Toestemming hebben de zorgkoepels met VWS 'gekozen' voor Mitz als online toestemmingsvoorziening, Het systeem is voor alle aangesloten systemen van zorgverleners een 'vertrouwd' beslissingpunt en bij iedere opvraging van gegevens zal Mitz worden geconsulteerd. De logging hiervan is effectief een gecentraliseerde database van alle behandelrelaties van alle patiënten in Nederland, ongeacht of ze zich hebben aangemeld bij Mitz.

Vervolgens vormt Mitz een *single point of failure*: compromittering van Mitz (of, potentieel, policy creep) maakt het mogelijk dat willekeurige aangesloten zorgverleners gegevens kunnen opvragen. Bij het uitvallen van het systeem, kunnen er geen gegevens meer worden uitgewisseld.

De categorale opzet van Mitz zorgt ervoor dat toestemmingen slechts een beperkte granulariteit hebben. Burgers geven met één toestemming duizenden zorgverleners (bijv. de categorie 'alle zorgverleners in de medisch specialistische zorg') toegang, en alle bronhouders in die categorie zullen hun gegevens moeten ontsluiten. Niet alleen wordt de zeggenschap van burgers hiermee drastisch ingeperkt, de zeggenschap over hoe zeggenschap is ingeregeld komt volledig bij de beheerders van Mitz te liggen, die met een druk op de knop het beleid kunnen aanpassen.

Doordat een gegeven toestemming direct geëffectueerd wordt, zónder tussenkomst van de bronhoudende zorgverlener, vallen een aantal waarborgen uit het gegevensbeschermingsrecht weg. Zo kan een zorgverlener niet meer verifiëren of het belang van derden niet wordt geschaad bij het delen van gegevens.

Een belangrijke vraag is bovendien in hoeverre burgers nog 'in vrijheid' toestemming kunnen geven voor deelname aan Mitz, wanneer een alternatief hiervoor ontbreekt.

Alternatieve methoden zijn al jaren bekend bij het Ministerie, zouden onderzocht gaan worden in het kader van de Wegiz[3], maar worden nu genegeerd. Ook binnen de NEN stuiten ideeën voor alternatieve methodes recentelijk op weerstand vanuit IZA partijen.

De IZA partijen hebben gekozen voor één centrale oplossing voor het registreren van toestemming: Mitz. Alternatieve ideeën zijn onbespreekbaar.

Lokalisatie

De huidige aanpak van het Ministerie is dat er één Landelijke 'Nationale VerwijsIndex' (NVI) komt. Hierin wordt centraal een lijst bijgehouden van patiënten en de zorgaanbieders die gegevens hebben over die patiënt (en ontstaat er een single point of failure). Mogelijk wordt ook hiervoor Mitz ingezet.

De NEN norm 7519/Lokalisatie beschrijft een meer generiek model voor lokalisatie, die niet alleen via een centrale index, maar ook binnen het zorgproces kan werken. Zo zou de huisarts over de tijd een verwijsindex kunnen opbouwen. Dat zou de huisarts (die een permanente behandelrelatie heeft met de patiënt) in staat stellen om meer dan alleen de 'eigen' gegevens beschikbaar te stellen bij een doorverwijzing, binnen de context van het medisch beroepsgeheim (zie bijlage). Zo wordt via standaardisatie voldaan aan het subsidiariteitsbeginsel, en ontstaan mogelijkheden om efficiënt en effectief lokalisatie gegevens te delen met *specifieke* bij de zorg betrokken zorgverleners, binnen het zorgproces.

Daarnaast kunnen burgers uiteraard alsnog (ook) Mitz of een LVI gebruiken om hun gegevens te lokaliseren. Dit vereist dan wel een uitdrukkelijke toestemming of minimaal een 'opt-out' mogelijkheid.

Autorisatie

Bij de (gecentraliseerde) autorisatie binnen een zorginstelling, wordt gekeken naar de rol (bijv. medische specialisatie) van de (mandaterende) zorgverlener om te bepalen welke gegevens inzichtelijk zijn. Vanwege de medische veiligheid heeft een grote groep zorgverleners (technisch) toegang tot gegevens, zonder dat ze deze (formeel) mogen opvragen. De verplichte behandelrelatie met de patiënt kan pas achteraf getoetst worden via logging.

FG's uit grote ziekenhuizen geven aan dat het toezicht op onrechtmatige bevragingen op een dergelijke schaal de grenzen van uitvoerbaarheid nu al overschrijdt.

---

[3] 27529, nr 189, 12 juli 2019, behandelrelatie als grondslag voor uitwisseling, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019D30926

Desondanks willen de IZA partijen dit model opschalen naar landelijk niveau, voor alle gegevens van iedereen. Autorisatieregels kunnen op basis van gezamenlijke afspraken aangepast worden zonder dat de verschillende zorgaanbieders dit zelf in hun systemen hoeven aan te passen. Doordat de leverancier dit implementeert hebben patiënt en arts geen zicht op en geen controle meer over welke gegevens met wie kunnen worden uitgewisseld

Ondanks juridische bezwaren en risico's voor de veiligheid en privacy blijven we geluiden horen dat het Ministerie koerst op '*autorisatie op zorgaanbieder-niveau*'. Hierbij wordt de opvragende partij verantwoordelijk voor de implementatie van autorisatieregels. Op basis van een landelijk 'afsprakenstelsel' (d.w.z. een gigantische gezamenlijke verwerkingsovereenkomst) kan een zorgaanbieder dan gegevens opvragen bij iedere andere zorgaanbieder. Een hack bij één zorgaanbieder is dan voldoende om van iedere patiënt in Nederland gegevens op te vragen via het Landelijk Dekkend Netwerk (LDN), waar ook Mitz en de NVI deel van gaan uitmaken. Deze aanpak is strijdig met state-of-the art, en de verantwoordelijkheden van zorgverleners/zorgaanbieders.

De functie autorisatie waar in NEN-verband generieke normen voor worden ontwikkeld, gaat uit van een flexibel gedistribueerd stelsel, waarin zorgaanbieders de autorisatieregels weliswaar vanuit een centraal punt kunnen downloaden, maar deze wel zelf kunnen controleren (en desgewenst aanpassen) voordat deze toegepast worden. Dit is van belang vanuit het perspectief van autonomie en zeggenschap van zorgaanbieders, zorgverleners en patiënten.

Adressering

Adressering wordt nu geleverd als centrale voorziening door VZVZ (ZorgAB)[4]. Deze voorziening kan een single point of failure vormen en biedt bovendien geen oplossing voor het managen van identiteitscertificaten van zorgaanbieders. Deze zijn nodig om de geldigheid van de adressen te kunnen controleren en de veiligheid van de verbinding met betreffende zorgaanbieders te kunnen valideren.

Een open (NEN) standaard voor adressering is aan te bevelen, gecombineerd met standaarden voor sleutelmanagement, om de zorginfrastructuur minder afhankelijk te maken van een centraal en kwetsbaar adresboek,. We zien nog geen beweging om een normeringsproces voor adressering op te starten, ondanks dat adressering wel als generieke functie geïdentificeerd is en er al een voorziening (ZorgAB) is.

[4] VZVZ, Vereniging van Zorgaanbieders voor Zorgcommunicatie, tevens leverancier van Mitz en het Landelijk SchakelPunt (LSP)

Conclusie

Beleid uit de -gesloten- governance van de IZA afspraken leidt tot een snelle uitrol van alles omvattende gecentraliseerde voorzieningen, met een impliciete overdracht van zeggenschap van burgers en zorgverleners naar de beheerders van die voorzieningen. In het tijdspad dat is uitgezet door de IZA-afspraken is er geen ruimte voor andere methodes en oplossingen en kan onmogelijk worden voldaan aan de subsidiariteitseisen.

Alternatieve methodes, zoals bekend bij het Ministerie en zoals beschreven in de NEN normen voor de 'generieke functies' worden genegeerd. Lopende NEN trajecten worden beïnvloed door beleidskeuzes van andere tafels die als voldongen feit worden gepresenteerd.

Dit is zorgelijk, omdat juist de open en transparante governance van de NEN zorgt voor diversiteit en inclusiviteit in de vertegenwoordiging van belangen, waaronder door burgerrechtenorganisaties. De NEN aanpak leidt tot openheid en interoperabiliteit van systemen en creëert ruimte voor meerdere methodes om medische gegevens beschikbaar te stellen (zowel gecentraliseerd als decentraal) waarmee kan worden voldaan aan ieders behoeften.

Vanuit burgerrechten perspectief is essentieel dat de NEN in haar rol erkend en versterkt wordt in het toekomstige stelsel, maar ook in de toekomstige governance rond de EHDS.