27 529 Informatie- en Communicatietechnologie (ICT) in de Zorg

Nr. 363 Brief van de minister van Langdurige Zorg, Jeugd en Sport

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 juni 2026

De vaste commissie voor Volksgezondheid, Welzijn en Sport heeft een brief ontvangen van Stichting Privacy First te Amsterdam d.d. 11 mei 2026 over “Commentaar Stichting Privacy First t.b.v. commissiedebat Digitale ontwikkelingen in de zorg d.d. 21 mei 2026” (zie bijgaande kopie). In de procedurevergadering van 27 mei 2026 heeft de commissie besloten een reactie van de minister op deze brief te willen ontvangen. Hierbij geef ik onderstaand mijn reactie en kom ik zo tegemoet aan het verzoek van de commissie.

Ik heb de brief van 11 mei 2026 waarin Stichting Privacy First (hierna Privacy First) aandacht vraagt voor de wijze waarop databeschikbaarheid in de zorg tot stand komt met belangstelling gelezen. De vragen die worden gesteld over privacy, transparantie, digitale veiligheid en zeggenschap raken direct aan fundamentele publieke waarden in de zorg.

Privacy First onderschrijft het belang van databeschikbaarheid, maar uit in de brief zorgen over de wijze waarop die databeschikbaarheid wordt vormgegeven. In de brief wordt gewaarschuwd voor de risico’s van ongerichte beschikbaarstelling van medische gegevens. Er wordt aandacht gevraagd voor een open en transparante governance, voor het behoud van zeggenschap bij de patiënt, voor de bescherming van het medisch beroepsgeheim van de zorgverlener en voor de risico’s voor privacy en digitale veiligheid van grootschalige centrale voorzieningen.

Ik ben het uiteraard volledig eens dat gegevensuitwisseling en databeschikbaarheid in de zorg nooit los kunnen worden gezien van privacybescherming, informatiebeveiliging, zeggenschap en publiek vertrouwen. Er worden in de brief echter ook enkele aannames gedaan die niet stroken met de laatste inzichten en stand van zaken binnen de projecten rondom gegevensbeschikbaarheid waar mijn ministerie aan werkt. Daarom acht ik het van belang om enkele beelden en conclusies uit de brief te nuanceren en op onderdelen te corrigeren.

Privacy First schetst het risico dat grootschalige gecentraliseerde voorzieningen zouden leiden tot een aantrekkelijk doelwit voor hackers, waarbij feitelijk “alles van iedereen” potentieel toegankelijk zou worden. Dat beeld herken ik niet. Het Landelijk Dekkend Netwerk (LDN) is geen centrale databank en ook geen voorziening waarin medische gegevens van alle Nederlanders worden samengebracht. Medische gegevens blijven in beginsel bij de bron: bij de zorgaanbieder of organisatie waar de data is

geregistreerd en waar de data onder verantwoordelijkheid van de bronhouder worden beheerd. Het LDN is bedoeld om, op basis van een landelijk afsprakenstelsel (LAS) en gecontroleerde toegang en inzage (de generieke functies), mogelijk te maken dat gegevens uit die verschillende bronnen beschikbaar kunnen komen wanneer dat noodzakelijk is binnen het zorgproces.

Daarmee wordt het door Privacy First geschetste beeld van een “one-stop-shop” voor hackers niet onderschreven. Een aanval op een functie of voorziening binnen het stelsel betekent niet dat alle medische gegevens van alle burgers op één plek beschikbaar zijn. Doordat gegevens bij de bron blijven, onder verantwoordelijkheid van de bronhouder worden beheerd én toegang via landelijke afspraken en generieke functies wordt begrensd, gecontroleerd, en herleidbaar gemaakt, ontstaat een gelaagde beveiligingsstructuur. De landelijke afspraken en generieke functies zoals uniforme beveiligingseisen (waaronder de NEN-7510), identificatie, authenticatie en autorisatie, toestemming, logging en toezicht zijn er specifiek op gericht de digitale weerbaarheid van de zorg te vergroten. Zoals ik ook in mijn recente Kamerbrief[1] over de voortgang van het Landelijk Dekkend Netwerk heb aangegeven: “Het gezondheidsinformatiestelsel wordt gerealiseerd op de fundamenten regie, vertrouwen en databeschikbaarheid.” Burgers, patiënten, zorgverleners en zorgaanbieders moeten erop kunnen vertrouwen dat gezondheidsgegevens veilig, betrouwbaar, rechtmatig, proportioneel en transparant worden gebruikt. Zonder dat vertrouwen kan digitalisering in de zorg haar maatschappelijke doel niet waarmaken.

Privacy First stelt daarnaast dat patiënten door digitale voorzieningen kunnen worden belast met keuzes die zij niet kunnen overzien. Ik neem het doenvermogen van burgers en patiënten serieus. Tegelijkertijd vind ik het te eenzijdig om daaruit te concluderen dat digitale regie in de zorg niet haalbaar of wenselijk zou zijn. In veel maatschappelijke domeinen nemen burgers inmiddels digitaal regie over zeer gevoelige informatie. Denk aan bankzaken, belastingzaken en pensioeninformatie. Ook daar gaat het om vertrouwelijke gegevens, financiële risico’s en afhankelijkheid van digitale infrastructuur. Dat vraagt om begrijpelijke informatie, veilige voorzieningen en goede ondersteuning, maar het uitgangspunt dat burgers digitaal geen betekenisvolle regie kunnen voeren, deel ik niet. Daarom wordt gewerkt aan Persoonlijke Gezondheidsomgevingen (PGO’s) en aan verdere ontwikkeling van de MGO-functionaliteit (Mijn Gezondheidsomgeving), zodat patiënten en burgers beter inzicht krijgen in hun eigen gezondheidsgegevens en beter in staat worden gesteld regie te nemen en te houden over hun gezondheid en de gegevens die daarbij horen. Ook is er een divers hulp- en ondersteuningsaanbod voor patiënten en burgers die nog niet beschikken over voldoende kennis, vaardigheden of middelen om

[1] Kamerstukken II2025/26, 27 529, nr. 361

digitaal regie te kunnen voeren over het delen van hun gezondheidsgegevens. Te denken valt hierbij aan initiatieven zoals Alliantie Digitaal Samenleven, Helpdesk Digitale Zorg en het programma Digivitaler dat via alle openbare bibliotheken beschikbaar kan worden gemaakt. Aanvullend is binnen de versnellingsagenda van de IZA/AZWA werkgroep Hybride Zorg door Patiëntenfederatie Nederland het thema digitale vaardigheden bij patiënten en zorgverleners geprioriteerd.

Privacy First stelt verder dat gerichte databeschikbaarheid in de zorg de standaard zou moeten zijn. In veel zorgprocessen ligt gerichte uitwisseling tussen specifieke zorgverleners voor de hand, bijvoorbeeld bij een verwijzing of overdracht binnen een planbare zorgsituatie of bijvoorbeeld wanneer een patiënt meetwaarden wil delen met een specifieke behandelaar. In andere situaties kan bredere beschikbaarheid noodzakelijk zijn om goede en veilige zorg te leveren, bijvoorbeeld wanneer een patiënt bij de spoedeisende hulp komt of in situaties waarbij relevante informatie uit meerdere bronnen nodig is. Daarom maak ik, naast gericht beschikbaar stellen, ook andere uitwisselingen mogelijk. Dat betekent echter niet dat voor deze uitwisselingsvormen andere of lichtere eisen gelden. Ook hier zijn privacy, doelbinding, autorisatie, logging, en navolgbaarheid randvoorwaardelijk – voor alle uitwisselingen gelden dezelfde, strikte eisen en data worden alleen onder voorwaarden raadpleegbaar gemaakt voor bevoegde partijen. Data raadpleegbaar maken is niet hetzelfde als het direct of daadwerkelijk delen, kopiëren of uitwisselen. De opgave is om het stelsel zo in te richten dat gegevensbeschikbaarheid situationeel, proportioneel en passend bij het zorgproces plaatsvindt. Daarbij moeten ontwerpkeuzes steeds worden getoetst aan noodzakelijkheid, proportionaliteit, subsidiariteit, uitvoerbaarheid en veiligheid.

De brief onderstreept terecht dat digitale veiligheid en transparantie geborgd moeten zijn. Recente incidenten en geopolitieke ontwikkelingen bevestigen dat dit blijvende aandacht vraagt. Vertrouwen en veiligheid ontstaan niet alleen door techniek en regelgeving, maar ook door navolgbare besluitvorming, duidelijke verantwoordelijkheden en betrokkenheid van relevante maatschappelijke perspectieven. Vanuit de Nationale visie en strategie vormen transparantie en openheid kernprincipes in de governance van het gezondheidsinformatiestelsel. In de recente Kamerbrief[2] heb ik aangegeven dat met het vernieuwde LDN-beleidsafwegingskader, er transparantie is en duidelijkheid blijft bestaan rondom de keuzes die bij de realisatie van het LDN worden gemaakt. Ook vanuit Europa wordt het belang van transparantie en verantwoording onderstreept. Zoals ik heb aangegeven in de EHDS-Kamerbrief[3] behoort dit tot een van de taken van een nog te

[2] Kamerstukken II2025/26, 27 529, nr. 361
[3] Kamerstukken II2025/26, 27 529, nr. 360

vormen zelfstandig bestuursorgaan (ZBO) die de Gezondheidsdata-autoriteit (GDA) zal heten.

Privacy First wekt in haar brief de indruk dat zijzelf (en/of andere burgerrechtenorganisaties) vooral aan de zijlijn staan van de ontwikkeling van het gezondheidsinformatiestelsel. Dat beeld behoeft correctie. De ontwikkeling van het stelsel vindt veelal plaats in een ‘community based’ proces waarin zowel zorg- en welzijnsperspectieven als maatschappelijke perspectieven zijn opgehaald en meegewogen. Denk hierbij aan werkgroepen en consultaties die mijn Ministerie faciliteert, alsook de NEN-normeringstrajecten waarvoor mijn Ministerie opdracht heeft gegeven. Stichting Privacy First is in dat proces wel degelijk meegenomen en heeft daarbij aan tafel gezeten. Dat betekent overigens niet dat iedere inbreng één-op-één is overgenomen. Het betekent wel dat zorgen over privacy, zeggenschap, transparantie en digitale veiligheid onderdeel zijn geweest van de inhoudelijke afwegingen.

Voor mij staat voorop dat vernieuwing van het zorgstelsel alleen verantwoord is wanneer zij plaatsvindt met behoud van maatschappelijk vertrouwen. Patiënten moeten kunnen begrijpen welke gegevens worden gebruikt, door wie, voor welk doel, onder welke voorwaarden en met welke rechten. Zorgverleners moeten kunnen vertrouwen op duidelijke kaders voor toegang, gebruik en verantwoording. Om die reden is vertrouwen één van de drie randvoorwaarden van de Nationale visie en strategie waaronder uitvoering wordt gegeven aan de totstandkoming van het gezondheidsinformatiestelsel. Daarbij zijn de Algemene Verordening Gegevensbescherming, het medisch beroepsgeheim, de relevante nationale wetgeving, Europese verplichtingen zoals de European Health Data Space, en geldende normen voor informatiebeveiliging, waaronder NEN-7510, kaderstellend. De verdere ontwikkeling van databeschikbaarheid in de zorg zal steeds plaatsvinden binnen duidelijke publieke kaders en met passende waarborgen voor patiënten, zorgverleners en instellingen.

Ik dank Stichting Privacy First voor haar bijdrage aan het debat.

De minister van Langdurige Zorg, Jeugd en Sport,
W.R.C. Sterk