

## **Interoperabiliteit van het NCPeH-NL**

In de Memorie van Toelichting (MvT) wordt onder 1.2 toegelicht dat in 2023 is gestart met de voorbereidingen voor de implementatie van de grensoverschrijdende zorgdienst patiëntsamenvatting A (PS-A)." Hierbij is niet vermeld dat voor deze patiëntsamenvatting alleen nog gegevens afkomstig uit huisartsensystemen worden gebruikt. Het lijkt nodig hierop in te gaan gezien de verschillen in standaardisatie van gegevens tussen bijvoorbeeld ziekenhuizen en huisartsenpraktijken, waardoor dit mogelijk nog geen maximaal herbruikbare patiëntsamenvatting betreft. Om verbetering van de patiëntsamenvatting met gegevens uit allerlei andere bronnen in de toekomst mogelijk te maken zonder onnodige extra inspanningen, is het cruciaal dat het nationaal contactpunt voor e-gezondheid in Nederland (NCPeH-NL) gegevens gaat kunnen verwerken op basis van dezelfde eisen die voor uitwisseling van deze gegevens binnen Nederland worden gesteld krachtens artikel 1.4 derde lid van de *Wet elektronische gegevensuitwisseling in de zorg (Wegiz)*. Een bepaling om dit te verzekeren ontbreekt in dit wetsvoorstel.

Hierbij lijkt het verstandig in de MvT in te gaan op de samenhang tussen de eis dat het NCPeH-NL gegevens converteert "naar het formaat van de betreffende zorgdienst" en de eis uit de EHDS dat een elektronisch patiëntendossier (EPD) een "interoperability component" bevat, waarvan in artikel 2 onder nc onder 2 al wordt vereist dat dit de gegevens oplevert in een voorgeschreven formaat. Als gegevens door een EPD in een voorgeschreven formaat worden opgeleverd aan het NCPeH-NL worden opgeleverd, lijkt er namelijk geen noodzaak meer te zijn om deze nog te converteren naar het voorgeschreven formaat en daarover bestaat al langer verwarring, die de bovengenoemde benodigde uitbreiding van de bronnen voor een patiëntsamenvatting tegenwerkt.

In de MvT wordt onder 3.2.3 gesteld dat ter identificatie van een patiënt naast het burgerservicenummer (BSN) de geboortedatum moet worden gebruikt. Een onderbouwing hiervan ontbreekt en gezien hiervoor binnen Nederland uitsluitend het gebruik van het burgerservicenummer (BSN) is voorgeschreven en in de structuur van dit nummer al de nodige controles zitten ter vermindering van risico's door bijvoorbeeld typefouten, lijkt dit niet triviaal. Ook dergelijke eisen beperken de mogelijkheden van EPD's om eenvoudig gegevensuitwisseling met het NCPeH-NL te realiseren en kunnen daarom grote impact hebben op de implementatie van grensoverschrijdende gegevensuitwisseling en dienen daarom te worden vermeden als hier geen zwaarwegende redenen voor zijn.

## **Authenticatie voor grensoverschrijdende gegevensuitwisseling**

In de MvT ontbreekt naar ons inzien enige toelichting. Authenticatie met betrouwbaarheidsniveau hoog zoals bedoeld onder 3.2.2 is pas haalbaar na inwerkingtreding van het wetsvoorstel voor *Wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Jeugdwet in verband met digitale identificatie en authenticatie in de zorg (DIAZ)*. Het lijkt daarom van belang deze afhankelijkheid te vermelden. Zolang de UZI-pas het enige authenticatiemiddel op dit niveau is, kan internationale gegevensuitwisseling niet goed en gebruiksvriendelijk in bestaande processen worden geïntegreerd. Dit is op deze manier dus ook wederom een beperking aan de interoperabiliteit van het NCPeH-NL.

### **Toestemming voor grensoverschrijdende gegevensuitwisseling**

In het wetsvoorstel is ook niets bepaald over onderscheid tussen toestemming voor gegevensuitwisseling binnen Nederland en voor grensoverschrijdende gegevensuitwisseling. In de MvT wordt gewezen op verschillen in de omgang met medische gegevens tussen lidstaten. Deze verschillen kunnen invloed hebben op het vertrouwen van burgers in de omgang met hun gegevens en daarmee op hun bereidheid hiermee in te stemmen. Om te vermijden dat de mogelijkheden voor grensoverschrijdende gegevensuitwisseling negatieve invloed hebben op de bereidheid van burgers om in te stemmen met gegevensuitwisseling binnen Nederland, lijkt het daarom van groot belang te bepalen dat burgers afzonderlijk van elkaar toestemming kunnen geven voor deze toepassingen.

In het verlengde hiervan kan worden overwogen een mogelijkheid toe te voegen om per land te bepalen of gegevens beschikbaar mogen worden gesteld aan zorgverleners die daar werkzaam zijn, wat burgers bovendien de mogelijkheid zou bieden geen toestemming te geven hun gegevens te delen met landen die zij niet bezoeken, om zo het risico op misbruik van hun gegevens te vermijden zonder grote impact op de kwaliteit van zorg die hen kan worden geleverd in landen waar zij wel komen. Hierbij is van belang dat artikel 8h van de voorgestelde *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space (EHDS)* zoals het Europees Parlement hiermee heeft ingestemd ([https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_EN.html)) niets zegt over het eventuele combineren van vragen om toestemming voor nationale en grensoverschrijdende gegevensuitwisseling en dit onderscheid dus enerzijds niet regelt maar anderzijds niet verbiedt.

### **Mitigatie van risico's van één enkel NCPeH-NL**

In het wetsvoorstel wordt geregeld dat persoonsgegevens mogen worden verwerkt. De vorm van deze verwerking is hierbij niet beperkt. Gezien het uitgangspunt dat er één en slechts één NCPeH-NL komt, op basis van artikel 12 tweede lid van de EHDS, lijkt dit het risico van een enorme 'privacy hotspot' op te leveren als dit NCPeH-NL bijvoorbeeld alle gegevens die hier passeren op zou gaan slaan. Hoewel uit de MvT goede intenties op dit vlak blijken, lijkt het verstandig ook expliciet in het wetsvoorstel op te nemen dat persoonsgegevens niet op een dergelijke manier door het NCPeH-NL mogen worden verwerkt (zonder dat daarvoor een aanvullende grondslag bestaat).

Om dezelfde reden lijkt het raadzaam het wetsvoorstel uit te breiden met eisen aan bijvoorbeeld de 'performance' en beschikbaarheid het NCPeH-NL of een mogelijkheid om dergelijke eisen te stellen bij Algemene Maatregel van Bestuur (AMvB) of Ministeriële Regeling (MR), om te vermijden dat dit 'single-point-of-failure' een te sterke beperking voor de toepassing van grensoverschrijdende gegevensuitwisseling op gaat leveren.