Een tweetal fundamentele opmerkingen en aanbevelingen over Wetsvoorstel 33509 (versie 1 juli 2014), Eric Verheul, hoogleraar Radboud universiteit en onafhankelijk adviseur technische informatiebeveiliging.

#	Context	Opmerking	Aanbeveling
1.	• Dit wetsvoorstel staat een centraal, elektronisch uitwisselingsysteem toe waar zich een Verwijsindex in bevindt. Deze Verwijsindex legt op basis van het Burgerservicenummer (BSN) vast in welke zorginformatiesystemen en bij welke zorgaanbieders patiëntgegevens liggen opgeslagen. • Het BSN wordt aldus gebruikt als gedeelde identiteit tussen het uitwisselingsysteem en de zorgaanbieders. Het BSN wordt ook gebruikt om burgers inzage te kunnen geven in de verwijsindex. • Ook het LSP van VZVZ [3.] beschikt over een dergelijke verwijsindex.	• Een dergelijke verwijsindex is ***onwenselijk*** en technisch ook ***niet noodzakelijk***. • ***Onwenselijk*** omdat de geschetste verwijsindex bijzonder privacygevoelig is. Immers, als hij bekend raakt dan wordt van alle Nederlanders duidelijk bij welke zorgaanbieder zij patiënt zijn. Dit zou het grootste privacy incident uit de Nederlandse geschiedenis zijn. De verwijsindex maakt een uitwisselingsysteem ook interessant voor cyberaanvallen. Met een buitgemaakte verwijsindex kan de Nederlandse maatschappij bijvoorbeeld gechanteerd worden. • ***Niet noodzakelijk*** omdat het relatief eenvoudig is om het BSN in de verwijsindex te pseudonimiseren. Hiervoor is in 2014 vanuit het Nederlandse eID stelsel ook reeds een cryptografische techniek ontwikkeld. Zie [1.]. Deze techniek kan bijvoorbeeld worden toegepast op het huidige LSP van VZVZ zonder dat er sprake hoeft te zijn van een verandering in diens functionele opzet maar waarbij de verwijsindex geen gevoelige persoonsgegevens meer bevat. Ook de inzage functie blijft ongewijzigd. Feitelijk kan op basis van bepaalde uitspraken [2.] van de Autoriteit Persoonsgegevens worden gemotiveerd dat het uitwisselingsysteem dan geen persoonsgegevens meer verwerkt. • Omdat het dus niet hoeft, *mag* het BSN dus ook niet worden verwerkt in het uitwisselingsysteem volgens het minimale gegevensverwerking beginsel (Artikel 5, aankomende Europese privacy verordening).	• Neem in het wetsvoorstel op dat een centraal uitwisselingsysteem alleen mag opereren op basis van gepseudonimiseerde gegevens conform de regels van de Autoriteit Persoonsgegevens [2.]. • Als alternatief kan bovenstaande ook als technische eis worden opgenomen in de algemene maatregel van bestuur (AMvB) op grond van artikel 26 Wbp zoals reeds voorzien in het wetsvoorstel. • Laat LSPs (waaronder dat van VZVZ) aansluiten op het Nederlandse eID stelsel.
2.	Bij het transport van patiënt data tussen zorgaanbieders via het VZVZ LSP [3.] komen deze data kortstondig in leesbare vorm beschikbaar in VZVZ uitwisselingsysteem.	• Deze opzet is ***onwenselijk*** en ook technisch ***niet noodzakelijk***. • ***Onwenselijk*** omdat dan via een beveiligingsbreuk in het uitwisselingsysteem patiëntgegevens in verkeerde handen kunnen komen. • **Niet noodzakelijk** omdat de gebruikelijke opzet is dat de verzendende partij de data zodanig versleuteld dat alleen de ontvangende partij deze kan ontsleutelen (publieke sleutel cryptografie). • Deze opzet wordt bijvoorbeeld ook toegepast bij het introductieplateau van het Nederlandse eID.	• Neem in het wetsvoorstel (of in de voorziene AMvB, zie vorig punt) op dat als het uitwisselingsysteem een actieve rol speelt in de uitwisseling van patiëntgegevens tussen zorgaanbieders, dat deze gegevens dan niet leesbaar mogen zijn voor dit systeem.

[1.]https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/documentatieset/PP_Scheme_091.pdf

[2.] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z2006-1382.pdf

[3.] https://www.vzvz.nl