Vragen n.a.v. Kennissessie NUTS:

1. ***Zit het aanmeldbericht in de scope van de regeling?***

Het aanmeldbericht hoeft niet worden uitgewisseld binnen het samenwerkingsverband. De deelnemers moeten echter wel het in werkproces zowel het aanmeld- als het overdrachtsbericht uitwerken (zie norm 5.2.f). Hierbij kijkt de auditor of er een procedure is omschreven en moet er a.d.h.v. een testcase de werkwijze worden gedemonstreerd. In het werkproces is er dus een onderscheid tussen aanmeld- en overdrachtsfase aantoonbaar, technisch wordt er getoetst op enkel het overdrachtsbericht.

Bij bovenstaande nog wel even de kanttekening dat de kaders voor de auditors nog nagelopen worden op eenzelfde consistentie (de toetsingskaders lijken daar enigszins anders verwoord).

2. ***Is NUTS ook geaudit op privacy en security en door wie?***

De Nuts node en de Nuts standaarden worden ontwikkeld en beheerd door bestaande leveranciers in de zorg ICT. De software draait onder hun verantwoordelijkheid en bestaande privacy en security audits. Daarnaast bestaat er wel de intentie om de node op termijn nog apart te laten valideren, wanneer de ontwikkeling (grotendeels) is afgerond. Anders schiet men op een bewegend doelwit.

In het ontwerp van de standaarden en de software zijn Privacy-by-design en security-by-design twee van de acht belangrijke pijlers van NUTS. In 2020 heeft Nuts de Dutch privacy award gewonnen:

> *"Voor de jury is stichting NUTS een mooi voorbeeld van een initiatief dat op een omvattende manier naar privacyvraagstukken kijkt en daar ook concrete oplossingen voor realiseert. De open source community die de stichting NUTS aan het realiseren is, voorkomt vendor-lock-in op cruciale onderdelen van de zorginfrastructuur. De in opkomst zijnde Persoonlijke Gezondheidsomgevingen kunnen eveneens gebruik maken van de decentrale beheersvoorzieningen die NUTS nastreeft. De gedachte achter NUTS – het creëren van een nutsvoorziening voor een cruciaal onderdeel van de zorgarchitectuur – spreekt de jury bijzonder aan."*

Zie hier.

3. ***Is er een lijst beschikbaar van leveranciers die meedoen met NUTS?***

Op www.nuts.nl staat een overzicht van leveranciers die actief Nuts uitdragen. Er zijn meer leveranciers betrokken, maar daar is geen totaaloverzicht van.

4. ***Zijn er überhaupt andere manieren dan NUTS om de eOverdracht vorm te geven?***

Het meest-voorkomende alternatief is het ontwikkelen van één op één koppelingen tussen leveranciers. Dit gebeurt nog regelmatig maar is onvoldoende schaalbaar en de beheerskosten zijn hoog. Bovendien zijn de datamodellen vaak niet standaard en zorgt dit voor extra afstemmingen.

5. ***Niet alle zorgpartijen (softwaresystemen) zullen tegelijk in NUTS zitten, misschien wel nooit. Hoe gaan de leveranciers deze situatie ondersteunen voor de gebruikers? Zodat je niet hoeft te gokken, meerdere processen moet weten. En waar ligt het zwaartepunt hiervoor? ECD, EPD,***

Broker, anders? Kan een leverancier of NUTS bestuur hier iets over zeggen? We zien nu een "happy flow"

Standaardisatie werkt alleen op het moment dat partijen eraan meewerken. Energieleveranciers moeten het er ook over eens zijn dat er 220 volt uit het stopcontact komt, zodat je apparaten kunnen werken. Dat is precies waarom de InZicht regeling bestaat: zorgen dat we allemaal dezelfde kant op bewegen. We hebben inmiddels ook alle leveranciers van ECD's in de langdurige zorg "mee", dus hopelijk volgt de rest ook snel.

6. ***Maar zolang niet alle HIS'en/ EPD's aansluiten, kan de versnippering verstorend werken in primaire proces. Dus daar moeten we wel wat mee, ook al zijn we op de goede weg.***

Eens, het is dan ook belangrijk dat vanuit de langdurige zorg de vraag geformuleerd blijft worden. En als het zich eenmaal heeft bewezen in de praktijk, gaat de sneeuwbal hopelijk verder rollen.

7. ***Hoe verhoudt het Zorg-AB (Adresboek) zich tot de adressering in NUTS?***

NUTS spreekt bewust van een Register en niet van een adresboek of adressering. Het verschil tussen het Register van NUTS en het Zorg-AB is de functie. Waar het ZorgAB een combinatie is van adressering en data van de geadresseerde (zoals KVK, AGB, UZI nummers), richt het Register van NUTS zich alleen op het adres en de service. In het Register van NUTS is de zorgorganisatie het beginpunt en vervolgens wordt middels endpoints gecontroleerd welke service er geleverd wordt (b.v. zorginzage of eOverdracht).
Inhoudelijk zit er weinig overlap tussen het ZorgAB en register; beide diensten kunnen dan ook goed naast elkaar bestaan. Omdat het Register decentraal functioneert (en de bron zelf aangeeft welke service/bolt er ondersteund wordt), betekent uitval bij een zorgorganisatie niet dat het Register verder niet bevraagd kan worden.
In het Nuts register verschijnen alle leveranciers en zorginstellingen die voldoen aan de technische Nuts standaarden. Het is dus een Register dat zich steeds verder zal vullen naarmate meer partijen de standaarden omarmen.

8. ***Hoe werkt de identificatie, hoe bepaalt NUTS de autorisatie, waar kunnen we de logging zien en wat moeten we daarmee doen?***

Authenticatie is het proces waarbij nagegaan wordt of iemand daadwerkelijk is die hij zegt te zijn. Het is het proces volgend op identificatie, waarbij de persoon zich kenbaar heeft gemaakt.
Authenticatie vindt momenteel vaak plaats tussen gebruiker en informatiesysteem. Als systemen onderling met elkaar communiceren, dan is de authenticatie van de gebruiker vaak niet meer te achterhalen (wel met een UZI-pas). Laat staan als dit over organisaties heen gaat.
NUTS wil garanderen dat er een veilige link is tussen: leverancier & zorgorganisatie, zorgorganisatie en gebruiker, leverancier en gebruiker en vereist hierbij een cryptografische handtekening. Uitgangspunt hierbij is dat elke organisatie zijn eigen zorgplicht heeft en zijn eigen applicaties met veilig opgeslagen data. De NUTS node valideert bij de eigen organisatie of de gebruiker is die hij zegt dat hij is en levert het bewijs naar de andere kant. Technische oplossingen die op een dergelijke wijze werken, zijn o.a. de UZI-pas of de IRMA app. De controle ligt dus in handen van de eindgebruiker. IRMA is een zogenaamde attribuut gebaseerde oplossing waarbij elke keer het bewijs dat uitgegeven wordt weer anders is of kan zijn. Het is dus niet een identifier gebaseerde oplossing (met bv. naam,

geboortedatum). Er is sprake van een cryptografische handtekening, op basis van de gehanteerde attributen. Dat betekent dat de handtekening elke keer uniek is.
Als aanbiedende partij van informatie, kan de identificatie gebruikt worden van het eigen systeem; de opvrager van informatie dient zich middels cryptografische handtekening kenbaar te maken. In de use-case van de eOverdracht van ziekenhuis naar thuiszorg, heeft het ziekenhuis als aanbiedende partij geen oplossing als IRMA nodig. Bij de thuiszorg is dit wel het geval, voor bijvoorbeeld de medewerkers die de overdracht ophalen. Omgekeerd geldt uiteraard hetzelfde. De transferverpleegkundige in het ziekenhuis kan IRMA gebruiken bij het opvragen van een overdracht, maar bijvoorbeeld ook de UZI-pas. NUTS ondersteunt technisch gezien ook de UZI-pas maar dit middel staat in de huidige vorm ter discussie. De gedachte voor de “nieuwe UZI pas” is ook gebaseerd op de attribuut gedachte en zou daarmee beter kunnen aansluiten bij NUTS.
Een middel als DigiD, dat werkt op basis van het BSN van de inloggende gebruiker, is voor deze toepassingen niet inzetbaar omwille van het feit dat de zorginstelling waar gegevens worden opgehaald geen juridische grondslag heeft om het BSN van een medewerker van een andere instelling te verwerken. Daarnaast zijn er praktische bezwaren en kosten waardoor DigiD geen zinnige bijdrage kan leveren aan uitwisseling tussen zorginstellingen.
De Autoriteit Persoonsgegevens (AP) stelt dat de authenticatiemiddelen in de zorg naar een hoog beveiligingsniveau moeten en hierbij moeten aansluiten bij Europese normeringen. Dit zal ook zo in de Wdo opgenomen worden. Nuts zal zich met het oog op de komende Wdo niet beperken tot een keuze in oplossingsrichting (IRMA) maar aansluiten bij de geldende wetgeving/Europese normeringen en als gevolg hiervan meerdere, erkende authenticatiemiddelen ondersteunen, zolang deze voldoen aan de gestelde eisen voor veiligheid en privacy.

Logging is niet een van de vier gemeenschappelijke voorziening zoals nu door het Informatieberaad Zorg is benoemd. Wel is logging voor NUTS een belangrijk onderwerp. De eisen die er worden gesteld aan logging zijn voor zorgorganisaties en leveranciers nu al duidelijk en zij moeten al aan deze eisen voldoen (veelal vastgelegd in de NEN 7513).
NUTS is echter bezig om specificaties op te stellen hoe je als patiënt/cliënt zelf gebruik kan maken van logging. Dit gebeurt om meerdere redenen:

1. De patiënt/cliënt wil je kunnen laten zien wat er gebeurd is met de data. Wie heeft welke informatie op welk moment ingezien.
2. Als plicht volgens de Algemene Verordening Gegevensbescherming (AVG).
3. Voor supportdoeleinden: omdat data zich in verschillende systemen bevindt, maakt logging het mogelijk om te zien waar welke data zich bevindt.

Door de patiënt/cliënt zelf inzage te geven in zijn logging, wordt ook voorkomen dat de (steeds mondiger wordende) patiënt/cliënt voor elk dataverzoek bij de zorgorganisatie aanklopt.
Logging gaat hand in hand met autorisaties. Autorisaties geven aan wie de logbestanden mag opvragen. In de logbestanden staan ook referenties naar autorisaties op basis waarvan uitwisselingen plaats hebben gevonden, zodat de rechtmatigheid daarvan kan worden bepaald.
NUTS denkt na of logging een kerncomponent van NUTS is of een aparte toepassing, een aparte bolt, moet zijn.

9. ***Waarom identificeren via een derde partij? Zou dit niet makkelijker kunnen via het netwerk van de zorginstelling? Bijvoorbeeld AD o.i.d.***
10. ***Wat is het verschil tussen regionaal en landelijk? Als ik ingelogd ben bij mijn ECD-leverancier zou dat voldoende moeten zijn. De leverancier is immers aangesloten en voldoet dus aan de eisen.***

Zorgverleners van de ene zorginstelling gaan gegevens ophalen bij de andere zorginstelling. Er worden dus personen geïdentificeerd die niet bij de organisatie werken. Dit kan alleen met de "eigen" inlogmiddelen (zoals AD) worden opgelost wanneer alle zorginstellingen in Nederland alle andere zorginstellingen en hun ICT-leveranciers vertrouwen. Omdat dat op landelijke, of zelfs Europese schaal geen haalbare ambitie is, leggen we deze verantwoordelijkheid bij een externe partij die we gezamenlijk vertrouwen. In dit geval het CIBG (via de UZI pas) of de vereniging Nederlandse gemeenten (via het IRMA attribuut).

11. ***Kan de Irma app wat de UZI pas kan?***

Zie ook het antwoord onder vraag 8. In principe zijn beiden authenticatiemiddelen bruikbaar waarbij de IRMA-app momenteel toegankelijker is dan de UZI-pas.

12. ***Het scannen van de QR-code in IRMA is niet een issue per se voor de zorgprofessionals (buiten dat intramurale zorgverleners veelal werk mobiel hebben) maar het verzamelen en verlopen van de attributen is een uitdaging. Ik zie daar een probleem met de uitleg naar zorgverleners. Zien anderen dat ook?***

Eens, dat is wel het minpunt van een SSI-wallet. Overigens verloopt een UZI pas ook na een jaar ofzo, en dat proces van vernieuwen is omslachtiger. Ik hoop dat a) gebruikers eraan wennen en b) we het steeds makkelijker/sneller/zeldzamer kunnen maken.

13. ***IRMA vereist een AGB-code, maar niet alle medewerkers hebben een AGB. Hoe kan je de IRMA app dan activeren?***

Zeker, voor eOverdracht maken we geen gebruik van het AGB-attribuut.

14. ***Klopt het dat je op de IRMA app in moet loggen met je digiD?***

Nee, je logt in de IRMA app in met een pincode. Je kunt wel met behulp van DigiD gegevens uit de gemeentelijke basisregistratie in de IRMA app laden, die we vervolgens kunnen gebruiken om mensen te identificeren. Dus we gebruiken indirect wel DigiD, maar dat hoeft maar eens per jaar om de attributen te vernieuwen.

15. ***Hoe weten we dan dat de zorgmedewerker Jan Jansen ook echt werkt bij Zorgorganisatie X en bij deze gegevens mag? En om te bewijzen dat Jan Jansen, Jan Jansen is moeten ze toch wel degelijk BRP gegevens ophalen met DigiD?***

Zoals bij de vorige vraag gesteld klopt het dat BRP gegevens met DigiD worden opgehaald. Dit gebeurt eens per jaar om de attributen te vernieuwen. We weten dat "Jan Jansen" bij zorgorganisatie X werkt doordat het verzoek om gegevens op te halen wordt gedaan door het ECD/EPD van zorgorganisatie X. De toegang van "Jan Jansen" op het eigen ECD/EPD is dus ook een onderdeel van de beveiliging van het Nuts netwerk. Verliest "Jan Jansen" toegang tot het eigen

systeem (bijvoorbeeld bij ontslag) dan verliest hij dus ook het vermogen om gegevens op het halen via het Nuts netwerk. Op termijn willen we dit proces zo gaan organiseren dat deze relaties actief door de zorginstellingen kunnen worden vastgelegd, zodat ook hier geen fraude meer mee kan worden gepleegd (voorbeeld door ECD/EPD leveranciers).

16. Is het eenmalig inloggen met je digID wel verplicht?

Dit is momenteel de enige manier om BRP attributen in de IRMA app te laden. Dus wanneer gebruik gemaakt wordt van de IRMA app dan is het inloggen met DigiD verplicht om de attributen op te halen of te vernieuwen. Er kan ook gebruik gemaakt worden van de UZI pas, wanneer niet hoeft te worden ingelogd met DigiD.

17. Is de pincode persoon of organisatie gebonden?

De pincode van de IRMA app is persoonsgebonden.

18. Maakt NUTS geen gebruik van digID voor de authenticatie?

Zie hierboven en vraag 8.

19. Welke attributen zijn dan wel nodig?

We gaan voor de eOverdracht gebruik maken van de attributen voornaam en achternaam uit de BRP en het attribuut e-mailadres van de zorgverlener. Dat laatste attribuut wordt afgegeven door SIDN, en vereist geen aparte koppeling met de systemen van de zorgverlener.

20. In NUTS is voorzien dat je bevestigt WIE je bent d.m.v. bijvoorbeeld IRMA. Daarbij wordt voor zover ik begrijp vooralsnog alleen het attribuut "Naam" vanuit de Basisregistratie Personen (BRP) gebruikt. Daarmee is niet geregeld dat je ook weet of die persoon daadwerkelijk (in een passende functie) voor de ontvangende Zorgorganisatie werkt. Het enige vertrouwen daarvoor is dat die persoon op dat moment is ingelogd/geautoriseerd in de applicatie van de Zorgorganisatie, maar is dat voldoende? Zou in IRMA/NUTS ook de relatie met de Zorgorganisatie niet vastgelegd moeten worden? En zo ja, levert dat dan weer onderhoud voor de Zorgorganisatie binnen NUTS op?

Dat is inderdaad een mooiere oplossing, en zoals al gesteld in vraag 15 werken we daar op termijn naartoe. Wanneer dat is gerealiseerd zal iemand in de zorginstelling de relaties moeten beheren (kan worden gevoed vanuit bestaande applicaties) en dit moeten accorderen met een cryptografisch middel, zoals op dit moment de IRMA app of UZI pas.
Voor de eOverdracht, op de korte termijn, is hiervoor gekozen omdat het op deze manier in dit stadium veilig genoeg is. De hoofdreden hiervoor is dat niet de zorgverlener, maar de zorginstelling de autorisatie ontvangt om een eOverdracht op te halen. Zodra de zorgverlener geen toegang meer heeft tot de systemen van de zorginstelling vervalt dus ook de mogelijkheid om die betreffende gegevens op te halen.

21. Dan is dit toch niet veiliger dan tweede factor georganiseerd door de werkplek?

Jawel, doordat de opvragende gebruiker herleidbaar is bij de aanbiedende zorginstelling, los van de account van de werkplek, is er een tweede laag van controle mogelijk. Wanneer we de relatie tussen

zorgverlener en zorginstelling ook vastleggen, zoals hierboven beschreven, is er niet alleen controle mogelijk maar kunnen we ook een hogere beveiliging afdwingen.

22. Hoe kan een zorginstelling medewerkers 'beheren' bij IRMA, zodat uitdiensttredingen tijdig worden verwerkt? Toegang tot gegevens is toch niet voor een persoon, maar voor een medewerker/functionaris van een bepaalde zorginstelling?

23. Is er beheer aan tabellen?

Zie vragen 15 en 20.

24. Wat ik niet geheel helder heb vanuit deze demo is of de gegevens die je binnenhaalt via de eOverdracht als zorgprofessional allemaal dan toch weer overgetikt moeten worden in een nieuw aan te maken zorgplan van de client die in zorg komt? Ik probeer even de eerste tijdswinst helder te krijgen voor het primaire proces zolang deze gegevens in deze fase nog niet gestructureerd als ZIB automatisch overgenomen wordt in het zorgplan.

Hier zit een onderscheid tussen de gestructureerde informatie, die via een ZIB wordt aangeleverd en de ongestructureerde informatie (via pdf/a). Voor de care-organisaties is onderdeel van de resultaatverplichting dat de 14 zib's wel degelijk ontvangen en verwerkt moeten worden in het ECD. En daarmee dus ook herbruikbaar zijn (= niet overtypen). De ongestructureerde informatie zal vooralsnog als pdf/a beschikbaar gesteld worden. Het is ook aan de leveranciers om zich aan deze resultaatverplichting te houden.
Zie ook de visuele weergave van de resultaatverplichting.

25. Wat merkt de eindgebruiker straks allemaal van NUTS?

Het is goed om te realiseren dat er een onderscheid is tussen NUTS en het gebruik van de standaard eOverdracht. NUTS richt zich zoals bekend op vier basiscomponenten: grondslag, logging, register en authenticatie. In het informatiesysteem (ECD) zal de eindgebruiker een keuze moeten maken voor een locatie/organisatie waarnaar overgedragen wordt. Verder zal de eindgebruiker 'geconfronteerd' worden met een toepassing om zich te authenticeren/identificeren. Zoals onder vraag 8 geschetst, geldt dit alleen voor de opvrager van informatie. Hij/zij gaat immers 'op bezoek' bij een andere organisatie en moet kunnen aantonen dat hij/zij is wie hij/zij zegt te zijn. Van de componenten logging en grondslag merkt de gebruiker niet veel, dat gebeurt onder water.

26. Kun je via ECD straks rechtstreeks naar/ via NUTS. Of ergens in een browser inloggen o.i.d.?

Hier merk je als eindgebruiker niks van en is geïntegreerd in het ECD. Leveranciers committeren zich aan een oplossingsrichting middels NUTS en zorgen ervoor dat deze techniek onderdeel wordt van de applicatie.

27. Hoe richt je binnen NUTS autorisaties in? Gelden bijvoorbeeld dezelfde rechten als binnen het ECD?

Dit hoeft niet apart ingericht te worden. Zoals geschetst onder 26, integreren leveranciers NUTS in hun ECD; deze rechten blijven overeind.

28. Als iemand uit dienst gaat hoe moet je dat wijzigen in NUTS?

Zie vragen 15, 20 en 26.

29. Komt er binnen het ECD een nieuw recht voor mensen die via NUTS gaan werken?

Dat is aan de leveranciers van de verschillende ECD systemen, maar het lijkt wel aannemelijk dat leveranciers een nieuw recht aan de applicatie zullen gaan toevoegen waarmee gericht gebruikers toegang gegeven kan worden tot de modules die betrekking hebben op de eOverdracht.

30. Hoe beschrijf je NUTS in je DPIA?

De impact van het gebruik van Nuts op de dataveiligheid ligt voor een deel ook aan de implementatie door de leverancier. Het is dus wijs om dit op te pakken in overleg met je leverancier.