HOOGHIEMSTRA & PARTNERS
strategisch en juridisch advies

Rapportage juridische vragen Nuts

Theo Hooghiemstra, Helen Hukshorn, Anna Keuning

Inhoudsopgave

Samenvatting

Steeds vaker wordt voor uitwisseling van patiëntgegevens tussen zorgaanbieders verkend of hiervoor gebruik gemaakt kan worden van Nuts. Vanuit de InZicht regeling en in aanloop naar de verplichtingen die de Wegiz stelt, moet in het kader van eOverdracht de gegevensuitwisseling tussen ziekenhuizen en VVT-instellingen en tussen VVT-organisaties onderling geregeld zijn. Om dit te realiseren, zijn er technische afspraken gemaakt. Ten eerste de afspraak dat Nuts de uitwisseling van ziekenhuizen naar VVT's veilig via het publieke internet laat verlopen. Ten tweede om de communicatie tussen VVT-organisaties uniform en eenduidig tot stand te brengen.

Naast de technische- en infrastructurele aanpassingen en eisen aan zorginformatiesystemen dragen de zorgaanbieders en zorgverleners ook de verantwoordelijkheid voor de bescherming van de medische gegevens. Die bescherming is gebaseerd op het medisch beroepsgeheim, patiënt toegang en -toestemming. In de praktijk blijkt dat er onduidelijkheid is over wat Nuts nu precies is, welke wettelijke eisen gelden en wat bij de inzet van Nuts nu de verantwoordelijkheden en verplichtingen zijn van de zorgaanbieders. Met name als het gaat om patiënttoestemming. In bijgaande analyse is ten eerste gekeken in hoeverre patiënttoestemming is vereist bij gebruik van Nuts door de zorgaanbieder. Daarnaast is gekeken óf en op welke wijze patiënttoestemming wordt geregeld en vastgelegd binnen Nuts. Dit is gedaan op basis van twee specifieke toepassingen: eOverdracht en Babyconnect. Vervolgens is een overzicht gegeven van de wettelijke vereisten die van toepassing zijn bij de inzet van Nuts en met welke toekomstige ontwikkelingen rekening moet worden gehouden. Tenslotte is gekeken naar de inzet van blockchain en privacy enhancing technologies binnen Nuts en naar de inrichting van de besturing en het toezicht binnen Nuts.

Wat is Nuts wel en wat is het niet?
In de praktijk zijn er veel misverstanden over wat Nuts wel en niet is. Voor de juridische analyse is het van belang hier, op hoofdlijnen, meer duidelijkheid over te krijgen. De Nuts community maakt en publiceert een open protocol dat het mogelijk maakt voor computers om met elkaar te kunnen communiceren, zoals het Internet Protocol. Een dergelijk protocol is vergelijkbaar met het protocol dat onder email ligt. Waar het internet ons in staat stelt anoniem met anderen te communiceren, zorgt Nuts ervoor dat de communicatie via internet niet langer anoniem is door een vertrouwenslaag aan het netwerk toe te voegen. De Nuts node vervult vier kernfuncties: identiteit en authenticatie, autorisatie (grondslag), register en logging. Door het open source protocol kan uitgewisseld worden tussen alle zorgaanbieders onafhankelijk van de gekozen leverancier. De communicatie hoeft daarmee niet beperkt te blijven tot de deelnemers die gebruik maken van hetzelfde platform of infrastructuur. Dit zónder dat er een derde partij nodig is die hier tussen zit.

Als de zorgaanbieder gebruik wil maken van Nuts, kan de leverancier van de zorgaanbieder op basis van de open source referentie implementatie die Nuts biedt, zelf een Nuts node inbouwen in de eigen applicatie. De node wordt aangesloten op het decentrale netwerk.
Als zorgaanbieders met elkaar willen gaan uitwisselen en Nuts willen gaan gebruiken voor een specifieke toepassing dan moeten zij daar onderling nadere afspraken over maken. Een specifieke toepassing werd voorheen "Bolt" genoemd, maar sinds kort gewoon "Toepassing op Nuts". Binnen de toepassing worden specifieke afspraken gemaakt door de zorgaanbieders die deelnemen.

Zorgaanbieders kunnen in de specifieke toepassing op Nuts afspreken dat Nuts toestemming gebruikt als grondslag. Deze toestemmingen worden echter niet in Nuts geregistreerd. De toestemming wordt geregistreerd in het bronsysteem van de zorgaanbieder en wordt meegegeven aan Nuts.

Met regelmaat wordt ten onrechte gedacht dat Nuts een toestemmingsvoorziening is die concurreert met Mitz. Nuts registreert geen toestemmingen en uit de analyse komt naar voren dat Nuts juist op termijn zou kunnen werken met toestemmingen die zijn geregistreerd in Mitz. Een ander misverstand is dat de patiëntgegevens uit het medische dossier ook via Nuts worden verstuurd. Dit is niet het geval, de daadwerkelijke uitwisseling van de patiëntgegevens vindt plaats via andere systemen van de zorgaanbieders. Nuts regelt alleen de vertrouwenslaag.

Als we bekijken wat bovenstaand betekent als het gaat om AVG-governance dan is op basis van de huidige informatie de conclusie dat de zorgaanbieder bepaalt dat men via het Nuts protocol wil gaan werken (middel) voor een specifieke toepassing (doel) en het open source protocol vervolgens laat inbouwen in de eigen omgeving. De zorgaanbieder bepaalt het doel en de middelen en is verwerkingsverantwoordelijke voor de verwerking die plaatsvindt. Nuts 'levert' slechts het protocol en heeft daarmee geen rol onder de AVG. De zorgaanbieder is daarmee verantwoordelijk voor het voldoen aan de verplichtingen die voortvloeien vanuit de AVG.

Een van de conclusies van dit rapport is dat het van belang is dat op een heldere wijze wordt gecommuniceerd over wat Nuts wel en niet is, met name voor doelgroepen zonder uitgebreide technische kennis zoals beleidsmakers, bestuurders en juristen. Op basis daarvan kunnen vervolgens afgewogen beslissingen worden genomen over het gebruik.

Patiënttoestemming vereist bij gebruik van Nuts door de zorgaanbieder? Op welke wijze wordt het vastgelegd binnen Nuts?
Er is niet één standaard antwoord mogelijk op deze vraag. Dat is afhankelijk van de wijze waarop de zorgaanbieders besluiten Nuts te gebruiken bij een specifieke uitwisseling en welke afspraken ze onderling maken over de vereiste grondslag. Als we kijken naar de geanalyseerde toepassingen, dan zie je dat dit kan verschillen. Bijvoorbeeld bij eOverdracht is sprake van een patiënt die wordt overgedragen naar een van te voren bekende andere zorgaanbieder, er is sprake van een doorverwijzing en daarmee kan gebruik worden gemaakt van veronderstelde toestemming.

Babyconnect is een vorm van netwerkzorg. Anders dan bij een eenmalige uitwisseling van gegevens zoals bij eOverdracht, vraagt netwerkzorg om een meer continu proces van inzagemogelijkheden, waarbij verschillende zorgaanbieders op verschillende momenten gegevens van elkaar moeten kunnen inzien en gebruiken. Bij de huidige gekozen inrichting en wijze van vragen van toestemming is op voorhand nog niet precies duidelijk, welke zorgaanbieders van het geboortenetwerk de zwangere nodig zal hebben en op welk moment. Er lijkt in de huidige vorm daarmee sprake te zijn van een elektronisch uitwisselingssysteem in de zin van artikel 15a Wabvpz. Als wordt gewerkt met een elektronisch uitwisselingssysteem dat de gegevens al van tevoren beschikbaar stelt, is de benodigde nadrukkelijke toestemming extra geregeld in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (artikel 15a lid 1 Wabvpz).

Het vastleggen van de patiënttoestemming vindt niet plaats in Nuts maar moet, door de zorgaanbieder worden geregistreerd. Op deze wijze kan men voldoen aan de aantoonplicht onder de AVG die geldt voor een verwerkingsverantwoordelijke die de grondslag toestemming gebruikt voor een verwerking. Het gebruik van Nuts verandert daarmee niks aan de bestaande situatie.

Huidige wet- en regelgeving en toekomstige ontwikkelingen
Als het gaat om de huidige wet- en regelgeving dan is een belangrijke conclusie dat deze met name van toepassing is op de zorgaanbieder. De zorgaanbieder moet voldoen aan de wettelijke vereisten vanuit de AVG, Wgbo, Wabvpz en eIDAS en moet daarmee ook zorgen dat de door hen gekozen toepassingen en software voldoen aan de gestelde eisen. Dit staat los van het gebruik van Nuts en geldt voor alle systemen die door de zorgaanbieder worden gebruikt.
Momenteel spelen verschillende ontwikkelingen die impact hebben op de wijze waarop gegevens tussen zorgaanbieders uitgewisseld worden en die daarmee impact kunnen hebben op Nuts.

Wegiz
De Tweede Kamer heeft het Wetsvoorstel gegevensuitwisseling in de zorg (Wegiz) in september 2022 unaniem aangenomen. Het wetsvoorstel wordt momenteel schriftelijk in de Eerste Kamer voorbereid. Zodra een gegevensuitwisseling geselecteerd wordt om verplicht elektronisch te verlopen dienen zorgaanbieders en ICT-leveranciers afspraken met elkaar te maken over de uitwisseling op het gebied van taal, techniek en ICT. Deze informatiestandaarden worden neergelegd in NEN-normen. De Verpleegkundige Overdracht staat bijvoorbeeld op de meerjarenagenda van de Wegiz. Daarvoor is recent een werkgroep ingesteld die de informatiestandaard NEN 7545 onder de Wegiz aan het ontwikkelen is.

EHDS
De Europese Commissie heeft op 3 mei 2022 de conceptverordening ‘Europese ruimte voor Gezondheidsgegevens’ (European Health Data Space – EHDS) gepubliceerd. De EHDS-verordening biedt een kader voor het elektronisch verwerken van gezondheidsgegevens voor drie doelen: het primair gebruik van zorgdata, het secundair gebruik van zorgdata en de ontwikkeling van een interne markt voor digitale gezondheidsproducten en -diensten, zoals EPD’s en gezondheidsapps. Bovendien bevat de EHDS bepalingen over de governance van data, zowel voor primair als secundair gebruik. Wat betreft primair gebruik gaat het daarbij grotendeels om dezelfde geprioriteerde gegevensuitwisselingen als bij de Wegiz. De meeste discussie over de EHDS vindt plaats over het secundair (hergebruik) van elektronische gezondheidsgegevens. Nuts is niet alleen toe te passen voor primair gebruik, maar ook voor secundair gebruik. Bij KiK-V (Keteninformatie Kwaliteit Verpleeghuiszorg) is Nuts al toegepast voor secundair gebruik.

Wet digitale overheid en toekomst UZI
De Eerste Kamer heeft op 21 maart 2023 de Wet digitale overheid (Wdo) aangenomen. De Wdo regelt nu enkel nog de situatie dat een burger of bedrijf wil inloggen op een digitale omgeving van een zorgaanbieder, en niet de situatie waarin digitale transacties tussen zorgaanbieders onderling plaatsvinden. De Wdo is een kaderwet met een flexibel karakter. Op die manier kan er ingespeeld worden op nieuwe ontwikkelingen. Het is daardoor goed mogelijk dat de Wdo in de toekomst ook het betrouwbaar inloggen tussen semi-publieke instellingen onderling zal gaan regelen, met een vergelijkbare acceptatieplicht van identificatiemiddelen.

Uit gesprekken met het programmateam Toekomstbestendig maken UZI komt naar voren dat het beleid voor de toekomst is dat in de zorg door professionals gebruik gemaakt kan worden van alle identificatiemiddelen die straks onder de Wdo geaccepteerd worden. Daarnaast wordt een vorm van certificering ontwikkeld waarbij onder voorwaarden ook middelen voor zorgprofessionals van grote zorgaanbieders worden geaccepteerd. Vooralsnog is nog geen sprake van een verplichting als het gaat om zorgprofessionals. Het is daarom raadzaam voor Nuts om in dit kader de nodige voorbereidingen te treffen zodat de implementatie van Nuts niet in de weg staat aan de acceptatie daarvan. Nuts schrijft in de basis geen specifiek identificatiemiddel voor, enkel dat het middel op cryptografische wijze aan validatie doet. Vanuit Nuts wordt ook aangegeven dat rekening wordt gehouden met deze ontwikkeling en meerdere middelen geaccepteerd zullen kunnen worden - naast Yivi (voorheen IRMA) - en nu nog de UZI-pas.

<u>eIDAS</u>
eIDAS staat voor 'Electronic Identities And Trust Services'. Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van deze verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. Dit kan alleen met een betrouwbare online identiteitscheck aan de voordeur.

Blockchain en cryptografie
Nuts maakt geen gebruik van Blockchain en hier is ook geen noodzaak toe. De reden dat er niet voor blockchain is gekozen, is dat bij Nuts geen consensus nodig is. Partijen publiceren alleen hun eigen publieke gegevens in het netwerk, er is dus geen sprake van potentieel conflicterende transacties en er hoeft dus ook niet tot consensus te worden gekomen.
Nuts maakt gebruik van cryptografische technieken. Gedurende de gehele gegevensverwerking via Nuts blijven de gegevens versleuteld. Het vertrouwensmodel van Nuts (identiteit, authenticatie en logging) is geheel vastgelegd in cryptografie. De hele vertrouwenslaag die Nuts is, is gebaseerd op de cryptografische principes van "ondertekenen", waarmee een stukje informatie in het netwerk altijd te koppelen is aan de oorspronkelijke auteur. Dit maakt het mogelijk een decentraal netwerk op te zetten, waarbij alle informatie te vertrouwen is. Binnen deze opdracht heeft geen audit plaatsgevonden op de cryptografie. Indien gewenst dient dit apart te worden uitgevoerd.

Governance Nuts netwerk
De governance van het Nuts netwerk is vergelijkbaar met de governance van het GSM-protocol. Nuts maakt gebruik van internationale open standaarden, Verifiable Credentials en Decentralized Identifiers en ontwikkelt haar governance door aan de hand van het internationale TrustOverIP vertrouwensmodel. Het kent daarmee geen centrale governance en toezicht, zoals bij ICT-infrastructuur in de zorg gebruikelijker is. Het voordeel is dat er geen sprake is van 'one point of failure.' Een nadeel is dat het lastiger te begrijpen is. Nuts lost dit op via een vertrouwensmodel op basis van cryptografie, laat hier audits op doen en is transparant over hoe hun model in elkaar zit.

1. Inleiding en werkwijze

1.1 Inleiding en juridische vragen

Het programma InZicht – Versnellingsprogramma gegevensuitwisseling Langdurige Zorg – is gericht op het stimuleren van de implementatie van de informatiestandaard eOverdracht tussen zorgorganisaties in de care (VVT en Gehandicaptenzorg) en met zorgorganisaties in de cure zoals ziekenhuizen. Tevens stimuleert InZicht de uitwisseling van de zorgorganisatie in de care met de cliënt.

Vanuit het InZicht programma en in aanloop naar de verplichtingen die de Wegiz stelt moet in het kader van eOverdracht de gegevensuitwisseling tussen ziekenhuizen en VVT-instellingen en tussen VVT-organisaties onderling geregeld zijn. Om dit te realiseren, zijn er technische afspraken gemaakt om met behulp van Nuts de uitwisseling van Ziekenhuizen naar VVT's veilig via het publieke internet te laten verlopen en om de communicatie tussen VVT-organisaties uniform en eenduidig voor Nederland tot stand te brengen.

Naast de technische- en infrastructurele aanpassingen en eisen aan zorginformatiesystemen dragen de zorgaanbieders en zorgverleners ook de verantwoordelijkheid voor de bescherming van de medische gegevens van (medisch beroepsgeheim), patiënt toegang en -toestemming. De grondslagen daarvoor zijn in diverse wetten, verordeningen en normen vastgelegd. In het kader van gegevensuitwisseling met behulp van het Nuts-netwerk bestaan onduidelijkheden over de verplichtingen van zorgaanbieders met betrekking tot patiënttoestemming. Daarnaast bestaan er onduidelijkheden over wat Nuts precies is en aan welke wettelijke eisen Nuts onderhevig is.

Om die reden heeft de Directie Langdurige Zorg (VWS) behoefte aan een juridische toets en inzicht in de randvoorwaarden met betrekking tot de bescherming van medische gegevens en patiënttoestemming bij gegevensuitwisseling met behulp van het Nuts-netwerk.

Na gunning van de opdracht is Hooghiemstra & Partners tevens gevraagd om het programma Babyconnect - een versnellingsprogramma voor informatie-uitwisseling tussen patiënt/cliënt en professional (VIPP) voor instellingen in de geboortezorg – mee te nemen in de analyse van de juridische vragen. Het doel van dit programma is naadloos aansluitende zorg voor moeder en kind(eren) rond de zwangerschap en geboorte. Dit is inclusief de overdracht naar andere zorgverleners van de cliënt en haar kind, waaronder de jeugdgezondheidszorg.

Hooghiemstra & Partners is gevraagd om de volgende vragen te beantwoorden:

A. Juridisch kader inzet Nuts

1. In hoeverre is patiënttoestemming vereist bij gegevensuitwisseling via Nuts, zelfs als er sprake is van doorverwijzing? Zo ja, hoe wordt patiënttoestemming binnen Nuts geregeld en vastgelegd?
2. Welke wettelijke vereisten zijn in het kader van gegevensuitwisseling van toepassing op Nuts?
3. Indien blockchain of andere cryptografische toepassingen binnen Nuts worden gehanteerd, welke eisen brengt dat mee ten aanzien van het gebruik van gegevens in de verpleegkundige overdracht?

4. In welke waarborgen moet worden voorzien ervan uitgaande dat niet alle wetten van kracht zijn (denk aan afspraken, convenanten e.d.)?

Bovenstaande vraag 1 ziet op de grondslagen voor gegevensuitwisseling (AVG, Wgbo, Wabvpz) bij de inzet van Nuts, met name als het gaat om de patiënttoestemming voor uitwisseling in verschillende mogelijke situaties (zoals doorverwijzing). Daarbij wordt meegenomen wat de vereisten zijn die gelden voor het vastleggen en aantonen van die toestemming (indien vereist).
Vraag 2 is breder en ziet op welke wettelijke vereisten verder gelden als het gaat om gegevensuitwisseling door middel van Nuts, daarbij wordt tevens vraag 4 meegenomen waarbij geanalyseerd wordt welke wetgeving nog niet van kracht is die wel impact heeft op de inzet van Nuts en tevens met welke toekomstige ontwikkelingen rekening moet worden gehouden (denk aan de Wegiz, Wdo, eIDAS, EHDS, herziening UZI). Bij de beantwoording van vraag 3 wordt bekeken welke juridische eisen en aandachtspunten gelden bij de inzet van blockchain en privacy enhancing technologies binnen Nuts ten aanzien van de uitwisseling van persoonsgegevens binnen de verpleegkundige overdracht.

B. Governance en waarborgen binnen Nuts community

5. Hoe is binnen de Nuts community de besturing inclusief externe toezicht georganiseerd?

Bij deze vraag wordt nader geanalyseerd op welke wijze de Nuts community is ingericht en met name op welke wijze de besturing vorm krijgt en het toezicht op de voorwaarden die gelden om aan te mogen sluiten bij de community (zowel intern als extern toezicht). Een analyse zal worden gemaakt van de huidige situatie tevens worden – indien relevant – aanbevelingen gedaan met betrekking tot de inrichting van de besturing en het toezicht, ook richting de toekomst.

1.2 Werkwijze

De onderzoeksvragen worden vanuit een juridisch perspectief beantwoord. Daarom zal slechts op hoofdlijnen worden beschreven hoe Nuts en de specifieke Nuts zorgtoepassingen in technische zin werken. Een analyse van de technische werking van Nuts valt buiten scope van deze analyse.

In de aanloop naar het opstellen van dit rapport is de aangeleverde documentatie geanalyseerd en is relevante wet- en regelgeving in kaart gebracht, inclusief toekomstige ontwikkelingen die van belang zijn voor de beantwoording van de vragen. Naast het literatuuronderzoek zijn er in deze fase semigestructureerd gesprekken gevoerd met de relevante partijen om de benodigde input op te halen. Er zijn gesprekken gevoerd met het bestuur van Nuts, met betrokkenen van het VIPP programma Babyconnect en met de betrokken wetgevingsjurist van VWS.

Vervolgens zijn de concept-bevindingen opgesteld en getoetst in een kick-off bijeenkomst met daarbij aanwezig zowel bestuurders als ontwikkelaars van Nuts, de opdrachtgever, betrokkenen van het programma InZicht en eOverdracht en betrokkenen van het ministerie van VWS. Vanuit VIPP Babyconnect was men verhinderd voor deze bijeenkomst. De deelnemers hebben de voorlopige bevindingen aangevuld en gecorrigeerd waar nodig. De kick-off zorgde voor extra inhoudelijke verdieping en een verkenning van waar nog vragen voor de toekomst liggen.

Op basis van het literatuuronderzoek, de interviews en de feedback uit de Kick-off meeting is een concept rapport opgesteld. Voor openstaande vragen zijn betrokken partijen benaderd om deze alsnog te kunnen beantwoorden. Daarnaast is in deze fase nog een interview geweest met betrokkenen van eOverdracht (nadere toelichting aanmeldbericht) én Babyconnect (nadere toelichting huidige inzet toestemming). Tevens is een overleg geweest met een vertegenwoordiger van het programma Toekomst UZI om te bezien op welke wijze dit van invloed is op de (toekomstige) inzet van Nuts. Het concept-rapport is voorgelegd aan de deelnemers aan de kick-off en vertegenwoordiging vanuit VIPP Babyconnect. Na verwerking van de opgehaalde feedback is het definitieve rapport opgesteld.

1.3 Leeswijzer

In hoofdstuk 2 wordt allereerst ingegaan op Nuts; wat is het wel en wat is het niet? In hoofdstuk 3 worden de algemene geldende kaders geschetst als het gaat om toestemming als grondslag en wordt beschreven welke rol onder de AVG de betrokken partijen hebben bij de inzet van Nuts. Vervolgens worden de beide toepassingen beschreven (eOverdracht en Babyconnect) en wordt vraag 1 beantwoord: in hoeverre is patiënttoestemming vereist bij de betreffende gegevensuitwisseling via Nuts, zelfs als er sprake is van doorverwijzing. Tevens wordt bekeken hoe patiënttoestemming binnen Nuts geregeld wordt en of deze binnen Nuts vastgelegd wordt. In hoofdstuk 4 wordt breder gekeken naar welke wettelijke vereisten verder gelden als het gaat om gegevensuitwisseling door middel van Nuts (vraag 2), daarbij wordt tevens vraag 4 meegenomen waarbij geanalyseerd wordt welke wetgeving nog niet van kracht is die wel impact heeft op de inzet van Nuts en tevens met welke toekomstige ontwikkelingen rekening moet worden gehouden. In hoofdstuk 5 wordt beschreven welke juridische eisen en aandachtspunten gelden bij de inzet van blockchain en privacy enhancing technologies binnen Nuts ten aanzien van de uitwisseling van persoonsgegevens binnen de verpleegkundige overdracht. In hoofdstuk 6 wordt nader geanalyseerd op welke wijze de Nuts community is ingericht en met name op welke wijze de besturing vorm krijgt en het toezicht op de voorwaarden die gelden om aan te mogen sluiten bij de community. Tenslotte volgt in hoofdstuk 7 de conclusie.

2 Wat is Nuts wél en wat is het niet?

Tijdens de analyse bleek dat het voor veel partijen lastig te 'vatten' is wat Nuts nu wel en niet is. Onderstaand een beknopte uitleg voor zover relevant voor de beantwoording van de juridische vragen.

2.1 Wat is Nuts wél?

De Nuts community[1] is een 'open source software ecosysteem.' De Nuts community maakt en publiceert een open protocol dat het mogelijk maakt voor computers om met elkaar te kunnen communiceren zoals het Internet Protocol (IP). Een dergelijk protocol is vergelijkbaar met het (SMTP) protocol dat onder email ligt. Als verzender kan je een ander emailprogramma gebruiken dan de ontvanger (bijvoorbeeld Gmail versus Outlook), draaiend op een ander besturingssysteem (bijvoorbeeld Windows versus iOS), gebruikmakend van een ander device (bijvoorbeeld laptop of tablet) en tóch komt een email aan en is het leesbaar voor de ontvanger. Er is dus sprake van een gedistribueerd netwerk, vergelijkbaar met het internet.

Waar het internet ons in staat stelt anoniem met anderen te communiceren, zorgt Nuts er voor dat de communicatie via internet niet langer anoniem is door een vertrouwenslaag aan het netwerk toe te voegen.
De Nuts-community bestaat uit softwareleveranciers in de zorg, met name de langdurige zorg, die samen werken aan dit open source protocol dat bruikbaar is binnen de zorg, waarbij het niet uitmaakt met welk ECD/EPD/XIS de data wordt opgevraagd of uitgewisseld.[2] De communicatie hoeft daarmee niet beperkt te blijven tot de deelnemers die gebruik maken van hetzelfde platform of infrastructuur, door het open source protocol kan uitgewisseld worden tussen alle zorgaanbieders onafhankelijk van de gekozen leverancier zónder dat hiervoor een derde partij nodig is die er tussen zit.

Nuts bestaat uit specificaties die zijn opgesteld door de Nuts-community, software en een netwerk. Nuts maakt onderscheid tussen zogenaamde **'nodes' en de 'Toepassing op Nuts'**. In de volgende twee paragrafen worden deze begrippen nader toegelicht.

2.1.1 De Nuts node

De Nuts node is de referentie-implementatie[3] van de Nuts specificaties. De documentatie van de Nuts node beschrijft hoe de node werkt en hoe je hieraan als ontwikkelaar kunt bijdragen.
Als een zorgaanbieder besluit Nuts te willen gebruiken als oplossing dan kan de leverancier van de zorgaanbieder op basis van de open source referentie implementatie die Nuts biedt, zelf een Nuts node inbouwen in de eigen applicatie. De node wordt aangesloten op het decentrale netwerk. De

[1] Community van partijen, met name ICT-leveranciers en Zorgaanbieders, die samenwerken aan de Nuts-specificaties, Nuts-referentieimplementatie en Toepassingen op Nuts. . Zie de definitie in de aansluitovereenkomst.
[2] ICTU, Impact Nuts binnen de VVE-sector, deel I. p. 10.
[3] Door Stichting Nuts via nuts.nl aangewezen software implementatie van de Nuts-specificaties. Zie de definitie in de aansluitovereenkomst.

nodes in het Nuts netwerk van de verschillende zorgaanbieders zijn in staat elkaar te vinden om met elkaar te communiceren. Het Nuts-netwerk is dus een verzameling Nuts-nodes van partijen die een aansluitovereenkomst met Stichting Nuts hebben afgesloten. De Nuts-node vervult vier kernfuncties (vertrouwenslaag) die te maken hebben met:

- Identiteit en authenticatie: Wie ben je? En kun je bewijzen dat je degene bent die je zegt te zijn? Nuts werkt nu met IRMA (vanaf begin april Yivi) voor het identificeren en authenticeren van de zorgprofessional maar kan ook werken met UZI. Vanuit Nuts wordt aangegeven dat op termijn ook met andere middelen kan worden gewerkt die voldoen aan de gestelde eisen in de zorg.
- Autorisatie: is er een grondslag, mag je de gegevens ophalen / inzien?
- Register: Waar kan ik je vinden? Via het Nuts-register kunnen de technische endpoints (API's) van andere aangesloten zorgaanbieders worden gevonden met wie je wilt uitwisselen.
- Logging: wie heeft op welk moment gegevens ingezien of opgehaald?

Hierbij is van belang als het gaat om gegevensbescherming dat de leveranciers in de community zich gecommitteerd hebben aan de uitgangspunten van het manifest van Nuts waaronder:

- Privacy by design: informatie wordt bewust met elkaar gedeeld door bijvoorbeeld het vastleggen van toestemmingen of de verzoeken tot het accepteren van informatie. Toestemmingen zitten dus in het ontwerp ingebakken.
- Security by design: beveiliging wordt in het fundament ingebouwd en er wordt uitgegaan van het feit dat er altijd partijen in het netwerk kunnen zijn die niet te vertrouwen zijn. Dit wordt ondervangen door dat data alleen benaderd kan worden op basis van een persoonlijke identiteit en verstrekte toestemming.
- Identiteit en toegang tot gegevens kent een cryptografische basis.[4]

2.1.2 Specifieke toepassingen op Nuts

Als zorgaanbieders met elkaar willen gaan uitwisselen en Nuts willen gaan gebruiken voor een specifieke toepassing (zoals eOverdracht en Babyconnect) dan moeten zij daar onderling nadere afspraken over maken. Binnen een specifieke "Toepassing op Nuts" (voorheen ook wel "Bolt" genoemd) worden specifieke afspraken gemaakt. Binnen de toepassing worden specifieke afspraken gemaakt door de zorgaanbieders die deelnemen (bvb over semantische standaarden, welke grondslagen worden geaccepteerd, hoe om te gaan met vastleggen grondslag door zorgaanbieder etc).

Voor het uitwisselen van gegevens van patiënten tussen zorgaanbieders is een grondslag nodig. Zoals bovenstaand beschreven moet dus per toepassing door de deelnemers worden vastgesteld – op basis van de daadwerkelijke inrichting – welke grondslag moet worden gebruikt en hoe deze toestemming door de zorgaanbieders wordt uitgevraagd bij de patiënt.

[4] ICTU, Impact Nuts binnen de VVE-sector, deel I. p. 10.

De Nuts specificaties zijn zo gemaakt dat – naast de grondslag toestemming – alle relevante grondslagen tot autorisaties kunnen leiden.

Als we kijken naar de documentatie van Nuts dan wordt een aantal 'vormen' van toestemming beschreven en ondersteund, afhankelijk van de gekozen inrichting door de zorgaanbieders:

- Expliciete toestemming (in termen van de AVG hebben we het dan over uitdrukkelijke toestemming);
- Veronderstelde toestemming (in geval van doorverwijzing);
- Wabvpz-toestemming vooraf (hier wordt gedoeld op de toestemming die geldt voor elektronische uitwisselingssystemen zoals opgenomen in art. 15a, eerste lid Wabvpz).

In hoofdstuk 3 wordt nader ingegaan op de algemeen geldende kaders als het gaat om toestemming als grondslag. Vervolgens worden de beide toepassingen beschreven (eOverdracht en Babyconnect) en wordt vraag 1 beantwoord: in hoeverre is patiënttoestemming vereist bij de betreffende gegevensuitwisseling via Nuts, zelfs als er sprake is van doorverwijzing.

2.2 Wat is Nuts niet?

Gedurende deze analyse is gebleken dat op een aantal terreinen misverstanden bestaan over wat Nuts is en wat het doet. Van belang voor het beantwoorden van de juridische vragen is om vast te stellen wat Nuts niet is.

<u>Uitwisseling patiëntgegevens vindt niet plaats via Nuts</u>

- Zodra via Nuts is vastgesteld dat de gegevens mogen worden uitgewisseld dan vindt de daadwerkelijke uitwisseling van de patiëntgegevens niet via Nuts plaats maar via andere systemen van de zorgaanbieder. Nuts heeft daar geen rol. Van belang is dus dat in de afspraken over de specifieke toepassingen tevens afspraken worden gemaakt die ervoor zorgen dat de verschillende systemen van de leveranciers die worden ingezet door de zorgaanbieders interoperabel zijn.
- De persoonsgegevens die tussen de betrokken Nuts-nodes worden uitgewisseld zitten in de autorisatie-records: het kan dan gaan om het BSN[5] en de informatie over de bronhouder en afnemers (waaruit de behandelrelatie tussen de persoon en de zorgaanbieder kan worden afgeleid).

<u>Nuts is géén toestemmingsregister</u>

Nuts is geen toestemmingsregister zoals bijvoorbeeld Mitz. In een toestemmingsregister (online toestemmingsvoorziening) kunnen de toestemmingen van patiënten (centraal) geregistreerd, geraadpleegd en beheerd worden.

Zorgaanbieders kunnen in de specifieke toepassing op Nuts afspreken dat Nuts toestemming gebruikt als grondslag. Deze toestemmingen worden echter niet in Nuts geregistreerd. De

[5] Afhankelijk van de toepassing op Nuts wordt bepaald welk attribuut nodig is om de autorisatie op te bouwen.

toestemming wordt geregistreerd in het bronsysteem van de zorgaanbieder en wordt meegegeven aan Nuts.

Door Nuts is aangegeven dat het technisch gezien ook mogelijk is dat zorgaanbieders afspreken dat Nuts gebruik maakt van toestemmingen uit toestemmingsregisters zoals het LSP en Mitz (dus toestemmingen gebruiken die zijn geregistreerd bij derde partijen en niet bij de zorgaanbieder zelf). Vanuit het programma Babyconnect is daarnaast aangegeven dat het in de praktijk ook zo wordt ingezet in de geboortezorg.

3 Toestemming als grondslag voor uitwisseling patiëntgegevens tussen zorgaanbieders

3.1 Algemeen: kader toestemming als grondslag voor uitwisseling

De patiënt moet erop kunnen vertrouwen dat informatie die hij of zij aan de zorgverlener verschaft niet zonder zijn of haar toestemming of zonder dat de wet het toestaat met anderen wordt gedeeld. Dit wordt gewaarborgd met het medisch beroepsgeheim. Deze plicht strekt er niet alleen toe de patiënt te beschermen op individueel niveau (privacy van de patiënt) maar dient ook het algemeen belang waar het gaat om de toegankelijkheid van de zorg (Artikelen 7:457 BW, 272 Sr, 218 Sv en 88 Wet BIG).
Wanneer er toestemming nodig is voor het uitwisselen van patiëntgegevens en wanneer niet, verschilt. De regels die daarbij gelden, liggen namelijk vast in verschillende wetten. Als het gaat om uitwisseling van patiëntgegevens tussen zorgaanbieders dan is dit voornamelijk geregeld in de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (U)AVG), de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO), en in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz). Onderstaand wordt kort ingegaan op wanneer toestemming vereist is en wanneer niet. Hierbij wordt ervan uitgegaan dat er geen sprake is van een wettelijke plicht of taak om uit te wisselen of van een vitaal belang. Voor een uitgebreidere toelichting zie ook Factsheet 'Toestemmingen voor het uitwisselen van medische gegevens tussen zorgverleners' | Brochure | Rijksoverheid.nl

3.1.1 Toestemming uitwisselen medische gegevens door zorgaanbieders: hoofdregel

- Hoofdregel: voor het doorbreken van het medisch beroepsgeheim is toestemming van de patiënt vereist (artikel 7:457, eerste lid, WGBO). Hierin is opgenomen dat de zorgverlener ervoor moet zorgdragen, dat aan anderen dan de patiënt geen inlichtingen over de patiënt dan wel inzage in of afschrift van de bescheiden, worden verstrekt dan met toestemming van de patiënt.
- Uit de AVG vloeit voort dat het hierbij gaat om uitdrukkelijke toestemming (art. 9, tweede lid, sub a). Uitdrukkelijke toestemming is een verzwaarde vorm van toestemming. Er worden tenslotte bijzondere persoonsgegevens verwerkt (gegevens over de gezondheid) en daarvoor geldt een verwerkingsverbod tenzij aan een van de voorwaarden in art. 9, tweede lid is voldaan. De doorbrekingsgrond voor het verwerkingsverbod is daarmee uitdrukkelijke toestemming en dat vormt tevens de grondslag voor verwerking onder de AVG (art. 6, eerste lid, sub a).

3.1.2 Eisen aan rechtsgeldige toestemming

De AVG stelt eisen aan deze uitdrukkelijke toestemming, artikel 7 AVG (vrijelijk, ondubbelzinnig, specifiek, geïnformeerd).[6]

[6] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#hoe-vraagt-u-toestemming-7524

Vrijelijk gegeven
De patiënt of diens wettelijke vertegenwoordiger mag niet onder druk worden gezet om toestemming te geven. Bovendien mag de patiënt of diens wettelijke vertegenwoordiger geen nadelige gevolgen ondervinden als er geen toestemming wordt verleend.

Ondubbelzinnig
Er moet sprake zijn van een actieve handeling. Bijvoorbeeld een (digitale) schriftelijke of een mondelinge verklaring. Het moet in elk geval volstrekt helder zijn dát er toestemming is verleend, door wie, wanneer, en waarvoor. Er mag niet uit worden gegaan van het principe 'wie zwijgt, stemt toe'. Het gebruik van voor-aangevinkte vakjes is dus niet toegestaan.

Geïnformeerd
De patiënt moet weten met welk doel de gegevens worden opgevraagd en/of verstrekt, wat de inhoud is van de informatie (welke gegevens) en moet de draagwijdte van zijn/haar toestemming kunnen overzien. De arts moet zich vóór het vragen van toestemming ervan vergewissen dat de patiënt hiervan op de hoogte is. Ook moet de patiënt worden geïnformeerd over het recht om de toestemming weer in te trekken. Deze informatie moet in een toegankelijke vorm worden aangeboden en moet begrijpelijk zijn.

Specifiek
Toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel. Als er sprake is van meerdere doeleinden dan moet de betrokkene hierover worden geïnformeerd en moet voor elk doel afzonderlijk toestemming worden gevraagd. Het doel mag niet gaandeweg veranderen.

3.1.3 Voorwaarde grondslag toestemming: aantonen dat toestemming is gegeven

Een belangrijke voorwaarde die de AVG stelt aan het gebruik van de grondslag toestemming, is dat de verwerkingsverantwoordelijke (in dit geval de zorgaanbieder) moet kunnen aantonen dat de patiënt toestemming heeft gegeven (artikel 7 lid 1 AVG). Dat staat los van het gebruik van Nuts of een andere voorziening of infrastructuur maar maakt deel uit van de verantwoordingsplicht die de verwerkingsverantwoordelijke onder de AVG heeft. Op welke wijze en door middel van welke handeling kan uitdrukkelijke toestemming onder andere worden aangetoond?[7]

Schriftelijke verklaring
Een voor de hand liggende manier om ervoor te zorgen dat toestemming uitdrukkelijk is, is het uitdrukkelijk bevestigen van toestemming in een schriftelijke verklaring. Om elke mogelijke twijfel en mogelijk gebrek aan bewijs in de toekomst te voorkomen, kan de verwerkingsverantwoordelijke de schriftelijke verklaring door de betrokkene laten ondertekenen. In de KNMG-richtlijn

[7] Idem.

‘Omgaan met medische gegevens’ wordt aangegeven dat schriftelijke toestemming weliswaar niet door de wet wordt voorgeschreven maar dat het in sommige gevallen verstandig kan zijn vanwege de aantoonbaarheid van de toestemming. [8]

Digitale of online context

In de digitale of online context kan een patiënt de vereiste verklaring verstrekken door het invullen van een elektronisch formulier, door het versturen van een e-mail, door het uploaden van een gescand document waarop de handtekening van de betrokkene staat, of door middel van een elektronische handtekening in het medisch dossier. Uitdrukkelijke toestemming kan ook worden verkregen via een website of zorgportaal door een scherm aan te bieden waarop selectievakjes "Ja" en "Nee" kunnen worden aangevinkt door een patiënt, mits de tekst duidelijk de toestemming verwoordt. De Autoriteit Persoonsgegevens geeft hierbij wel aan dat alleen verwijzen naar de automatische registratie via de website onvoldoende is; dit kan bijvoorbeeld worden gecombineerd met documentatie over het proces waarin is vastgelegd op welke manier u toestemming ontvangt en vastlegt plus een kopie van de informatie die de betrokkenen hebben ontvangen voorafgaand aan de gegeven toestemming.

Mondelinge verklaring

In theorie kan het gebruik van mondelinge verklaring ook voldoende zijn om geldige uitdrukkelijke toestemming te verkrijgen, het kan echter voor de verwerkingsverantwoordelijke moeilijk te bewijzen zijn dat voldaan is aan alle voorwaarden voor geldige uitdrukkelijke toestemming.

3.1.4 Uitzonderingssituaties

- Het beroepsgeheim geldt niet tegenover hulpverleners die *rechtstreeks betrokken* zijn bij uitvoering van dezelfde behandelingsovereenkomst. Dan kunnen de noodzakelijke gegevens worden gedeeld. Te denken valt aan personen die de arts bij zijn werkzaamheden assisteren, zoals verpleegkundigen, doktersassistenten en diëtisten. Maar onder de rechtstreeks betrokkenen valt ook de collega-vakgenoot aan wie advies wordt gevraagd in het kader van de behandeling. En de patholoog die op verzoek van de behandelend arts weefsel van een patiënt beoordeelt.
- Als een hulpverlener een patiënt *doorverwijst* dan mag toestemming van de patiënt worden verondersteld. Omdat de patiënt instemt met de verwijzing, wordt verondersteld dat hij ook instemt met de informatie-uitwisseling. De patiënt moet wel geïnformeerd worden door de hulpverlener.

3.1.5 Uitwisselen via een elektronisch uitwisselingssysteem: uitdrukkelijke toestemming

In paragraaf 2.2.1 is aangegeven dat uit de Nuts documentatie blijkt dat ook de Wabvpz-toestemming vooraf kan worden ondersteund als dit vereist wordt door een specifieke toepassing.[9] Over de Wabvpz-toestemming is veel verwarring. (hier wordt gedoeld op de toestemming die geldt voor elektronische uitwisselingssystemen zoals opgenomen in art. 15a, eerste lid Wabvpz). Bij deze

[8] KNMG-richtlijn, Omgaan met medische gegevens, p. 19.

[9] Momenteel is nog geen toepassing op Nuts die werkt met een Wabvpz-toestemming.

systemen worden de gegevens van de patiënt al van tevoren beschikbaar gesteld door de zorgverlener die deze gegevens heeft. De zorgverlener zorgt er dan voor dat de gegevens over de patiënt al beschikbaar zijn zodat een nog onbekende zorgverlener ze kan raadplegen indien noodzakelijk. Een voorbeeld van een elektronisch uitwisselingssysteem is het Landelijk Schakelpunt (LSP).
Voor het beschikbaar stellen van de gegevens heeft de zorgverlener al uitdrukkelijke toestemming nodig want het beroepsgeheim wordt tenslotte verbroken (andere zorgverleners kunnen toegang krijgen en de zorgverlener die verantwoordelijk is voor de medische gegevens heeft geen controle meer over wie toegang krijgt). Als wordt gewerkt met een elektronische uitwisselingssysteem dat de gegevens al van tevoren beschikbaar stelt, is de benodigde nadrukkelijke toestemming extra gewaarborgd in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (artikel 15a lid 1 Wabvpz). Als deze toestemming er niet is, is uitwisseling niet mogelijk aangezien de gegevens dan niet in het systeem beschikbaar mogen zijn. Dit betekent dan ook dat er géén uitzonderingen mogelijk zijn zoals bijvoorbeeld veronderstelde toestemming bij een doorverwijzing. Voor de zorgverlener die de gegevens vervolgens wil raadplegen, geldt uiteraard dat dit alleen kan als dit noodzakelijk is voor de behandeling van de betreffende patiënt en de patiënt uitdrukkelijk heeft ingestemd met het delen van de gegevens. Ook de ‘nieuwe’ zorgaanbieder heeft een grondslag nodig voor het inzien van de beschikbare gegevens.

3.2 AVG-rollen bij inzet Nuts

In termen van de AVG is de natuurlijke persoon of rechtspersoon die het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt, de verwerkingsverantwoordelijke (artikel 4 lid 7 AVG). De verwerkingsverantwoordelijke is verantwoordelijk voor het treffen van passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd (art. 24 AVG).) De verwerker is een natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke (namens) persoonsgegevens verwerkt (artikel 4 lid 8 AVG). Deze partij dient de instructies van de verwerkingsverantwoordelijke op te volgen (artikel 28 AVG lid 3).

Alhoewel het geen deel uitmaakt van de juridische vragen is het zonder de AVG-rollen van partijen te analyseren niet mogelijk de vragen te beantwoorden. Daarom een beknopte analyse hiervan vooraf. Bij Nuts zijn vier (mogelijke) situaties te onderscheiden:

1. Een partij verwerkt geen persoonsgegevens en bepaalt ook niet doel en middelen van een partij die dat wel doet;
2. Een partij verwerkt persoonsgegevens, maar doel en middelen worden door een andere partij bepaald;
3. Een partij verwerkt persoonsgegevens en bepaalt a) doel en middelen van de verwerking van persoonsgegevens, al dan niet b) gezamenlijk met anderen;
4. Een partij verwerkt geen persoonsgegevens, maar bepaalt wel doel en middelen van de verwerking van persoonsgegevens door een andere partij, al dan niet gezamenlijk met derden.

In situatie 1 heeft desbetreffende partij geen verantwoordelijkheden onder de AVG. In situatie 2 is die partij een verwerker en zal passende technische en organisatorische maatregelen moeten

treffen om de verwerking afdoende te beveiligen (artikel 32 AVG) en zal ook passende afspraken moeten maken over de instructiebevoegdheden van de partij die doel en middelen van de verwerking bepaalt (artikel 28 AVG).

In situaties 3 en 4 is die partij een verwerkingsverantwoordelijke in de zin van artikel 4 lid 7 AVG en heeft daarbij de verantwoordelijkheid voor het aantoonbaar treffen van passende technische en organisatorische maatregelen om de verwerking in overeenstemming met de AVG te waarborgen (artikel 24 AVG). Als er sprake is van gezamenlijke verwerkingsverantwoordelijkheid moeten er op grond van artikel 26 AVG ook onderlinge afspraken zijn tussen de verwerkingsverantwoordelijken over het waarborgen van de rechten van betrokkenen.

In de context van Nuts zijn de zorgaanbieders de verwerkingsverantwoordelijke als het gaat om de uitwisseling van patiëntgegevens met andere zorgaanbieders. Zij bepalen het doel van en de middelen voor de verwerking van de gegevens als het gaat om de uitwisseling binnen een specifieke toepassing.

Voor de leveranciers van de zorgaanbieder is - afhankelijk van de gekozen constructie of technische oplossing - zowel mogelijk dat de leverancier een verwerker is van de zorgaanbieder óf slechts een leverancier van software die door de zorgaanbieder wordt gebruikt. In het laatste geval heeft de leverancier geen rol onder de AVG.

Nuts is een open protocol dat het mogelijk maakt voor computers om met elkaar te kunnen communiceren. Als een zorgaanbieder besluit Nuts te willen gebruiken als oplossing dan kan de leverancier van de zorgaanbieder op basis van de open source referentie-implementatie die Nuts biedt, zelf een Nuts node inbouwen in de eigen omgeving. Als zorgaanbieders ervoor kiezen om met elkaar te gaan uitwisselen en Nuts willen gaan gebruiken voor een specifieke toepassing dan moeten zij onderling nadere afspraken maken over semantische standaarden, welke grondslagen worden geaccepteerd, hoe om te gaan met vastleggen grondslag door zorgaanbieder etc). Op basis van het open source protocol kan uitgewisseld worden zónder dat er een derde partij tussen zit.

Op basis van de informatie die in het kader van deze opdracht is verstrekt, is de conclusie dat de zorgaanbieder bepaalt dat men via het Nuts protocol wil gaan werken (middel) voor een specifieke toepassing (doel) en het open source protocol vervolgens laat inbouwen in de eigen omgeving. De zorgaanbieder bepaalt het doel en de middelen en is verwerkingsverantwoordelijke voor de verwerking die plaatsvindt. Nuts ‘levert’ slechts het protocol en heeft daarmee geen rol onder de AVG.

3.3 eOverdracht en Nuts

3.3.1 Beschrijving toepassing eOverdracht

Vanuit het InZicht programma en in aanloop naar de verplichtingen die de Wegiz stelt moet in het kader van eOverdracht de gegevensuitwisseling tussen ziekenhuizen en VVT-instellingen en tussen VVT-organisaties onderling geregeld zijn. Om dit te realiseren, zijn er technische afspraken gemaakt om via Nuts de uitwisseling van Ziekenhuizen naar VVT’s te laten verlopen en om de communicatie tussen VVT-organisaties uniform en eenduidig voor Nederland tot stand te brengen.

Het gaat hierbij dus om een patiënt die van de ene zorgaanbieder wordt overgedragen naar een andere zorgaanbieder omdat vervolgzorg noodzakelijk is (ziekenhuis naar VVT).

Proces eOverdracht via Nuts op hoofdlijnen op basis van de beschrijving in de leverancierssspecificatie van de Toepassing op Nuts eOverdracht: [10]

Fase 1: Aanmelden patiënt bij andere zorgaanbieders; doel is om een zorgaanbieder te vinden die de vervolgzorg op zich kan nemen:

Het aanbieden van de patiënt aan andere organisaties kan plaatsvinden door het beschikbaar stellen van een aanmeldbericht. In dit aanmeldbericht staan die gegevens uit het dossier van de patiënt die relevant zijn voor de plaatsing. Het doelsysteem van de organisatie ontvangt een event of notificatie dat er een nieuw aanmeldbericht klaarstaat, en kan dit aanmeldbericht ophalen en tonen aan de gebruiker. De gebruiker kan dan namens de ontvangende zorgorganisatie geïnformeerd de keuze maken om de patiënt te accepteren of te weigeren. Het aanmeldbericht is bedoeld om vraag een aanbod bij elkaar te brengen. Welke informatie daadwerkelijk in het aanmeldbericht staat is aan de verzendende organisatie. Deze moet daarbij in overweging nemen in welke context het aanmeldbericht gebruikt wordt; is al vastgesteld dat de patiënt naar de betreffende ontvangende organisatie wordt overgeplaatst op basis van afstemming die al eerder heeft plaatsgevonden via een andere route (Zorgdomein, Point, mail, telefoon etc) of is daar nog geen sprake van?

Fase 2: Daadwerkelijke overdracht van de patiënt aan een andere zorgaanbieder:

Één zorgaanbieder is bereid gevonden om de patiënt over te nemen, de patiënt is daarover geïnformeerd en is akkoord.

De overdracht wordt geregistreerd in het bronsysteem (zorgaanbieder waar de patiënt is), waardoor een overdrachtsbericht beschikbaar wordt gesteld aan het doelsysteem (zorgaanbieder waar de patiënt naartoe gaat). In het overdrachtsbericht staat het relevante deel van het dossier van de overgedragen patiënt. Het doelsysteem ontvangt hier een notificatie van. De leverancier van het doelsysteem kan de zorgaanbieder (de gebruiker) waar de patiënt naartoe gaat notificeren dat er gegevens beschikbaar zijn.

Tenslotte kan de gebruiker zichzelf identificeren met een cryptografische handtekening en namens haar organisatie de dossiergegevens van de betreffende patiënt ophalen bij het bronsysteem. De medische gegevens worden dan zoals eerder aangegeven niet uitgewisseld via Nuts maar door de systemen van de zorgaanbieders. In de leverancierssspecificatie wordt aangegeven dat de overdragende partij hiermee kan voldoen aan haar logging-eisen met betrekking tot de NEN7513. Wanneer de ZIBs naar behoefte zijn opgehaald kunnen ze het startpunt vormen voor de intake van de patiënt en diens voortgezette behandeling bij de nieuwe zorginstelling.

[10] https://nuts-foundation.gitbook.io/bolts/eoverdracht/leverancierssspecificatie

In het ontwerp van deze toepassing wordt dus uitgegaan van een notified pull. Dit houdt in dat gegevens niet actief gestuurd worden naar het doelsysteem (push) en dat het doelsysteem niet lukraak gegevens ophaalt (pull). In plaats daarvan stuurt het bronsysteem een notificatie naar het doelsysteem dat er specifieke gegevens klaar staan om opgehaald te worden. Alleen naar aanleiding van die notificatie haalt het doelsysteem de benodigde gegevens op.

In de leverancierssspecificatie wordt aangegeven dat het voordeel van deze aanpak boven push is dat het doelsysteem gegevens alleen dan op hoeft te halen wanneer de ontvangende partij ook daadwerkelijk behoefte aan deze gegevens heeft. Op deze manier kan dus beter aan de eis van dataminimalisatie worden voldaan. Ook is het eenvoudiger om vast te stellen dat de persoon die gegevens ophaalt de juiste persoon is, en om te voldoen aan de NEN7513 en AVG verplichting om te loggen welke persoon de gegevens heeft ingezien.

3.3.2 Is patiënttoestemming vereist?

Fase 2: overdracht van de patiënt

Bij de verpleegkundige overdracht wordt een patiënt van de ene zorgaanbieder, naar de andere zorgaanbieder overgedragen. Bijvoorbeeld van een ziekenhuis naar een verpleeghuis. De noodzakelijke medische gegevens van de patiënt worden dan tevens overgedragen aan de 'nieuwe' zorgaanbieder. Welke gegevens noodzakelijk zijn, is vastgelegd in de Informatiestandaard eOverdracht. Hier is dus sprake van uitwisseling met een derde partij en daarvoor is patiënttoestemming vereist.

Echter, een overdracht van een patiënt is in feite een doorverwijzing. Met de patiënt wordt besproken welke vervolgzorg nodig is, de patiënt wordt geïnformeerd en gaat akkoord met de overdracht naar een specifieke bij de patiënt bekende zorgaanbieder. Hierbij kan dus worden uitgegaan van veronderstelde toestemming. Gezien de patiënt om toestemming is gevraagd om overgedragen te worden en ook is geïnformeerd over deze overdracht en naar wie, is het voorzienbaar voor de patiënt dat zijn gegevens daarbij ook worden overgedragen. Hoewel deze vorm van toestemming niet in de WGBO of (U)AVG is opgenomen, wordt deze in de literatuur wel erkend als een geldige vorm van toestemming.

Elektronisch uitwisselingssysteem?
Bij de gekozen werkwijze bij eOverdracht is sprake van notified pull. Niet te verwarren met de pull die plaatsvindt binnen een elektronisch uitwisselingssysteem. Bij een elektronisch uitwisselingssysteem worden patiëntgegevens beschikbaar gesteld door de zorgverlener zodat een nog onbekende zorgverlener ze kan raadplegen indien noodzakelijk. Bij eOverdracht is sprake van een één op één overdracht waarbij vooraf bekend is welke zorgaanbieder de gegevens zal opvragen. Er is dus geen sprake van een elektronisch uitwisselingssysteem en art. artikel 15a lid 1 Wabvpz Staat daarmee niet in de weg aan uitwisselen op basis van veronderstelde toestemming bij een doorverwijzing.

Fase 1: Aanmeldbericht

In de leverancierssspecificatie eOverdracht staat beschreven dat nadat op hoofdlijnen bekend is naar welke zorgaanbieders de patiënt kan worden overgedragen, een notificatie wordt verstuurd aan de

betreffende zorgaanbieders dat er een aanmeldbericht klaar staat. Net zoals de medische gegevens van de overdracht zelf wordt ook het aanmeldbericht niet via Nuts verstuurd, maar via de infrastructuur tussen de zorgaanbieders. Er is een informatiestandaard vastgesteld voor het aanmeldbericht (Opbouw eOverdracht aanmelding v3.1).[11]

Zorgaanbieders kunnen nu nog zelf bepalen of en hoe ze een aanmeldbericht versturen. Dat kan dus zowel met als zonder persoonsgegevens zijn. Dat gebeurt nu veelal nog op andere manieren zoals via bestaande marktpartijen die fungeren als tussenpartij.

Aandachtspunten voor toekomstige inzet:

- Er wordt aangegeven dat het ook mogelijk is om een aanmeldbericht te versturen zonder dat deze persoonsgegevens bevat. Uit de informatiestandaard blijkt dat er persoonsgegevens in zijn opgenomen. Indien ernaar wordt gestreefd het aanmeldbericht te anonimiseren (indien mogelijk heeft dit de voorkeur) zal zorgvuldig onderzocht moeten worden of er ook daadwerkelijk sprake is van anonimisering.
- Als een aanmeldbericht mét persoonsgegevens wordt verstuurd door de zorgaanbieder naar verschillende andere zorgaanbieders om te bepalen of er een match is, is sprake van uitwisseling van medische gegevens met een derde partij. Hierbij kan nog niet worden uitgegaan van een doorverwijzing en uitdrukkelijke toestemming van de patiënt is vereist.
- Het heeft de voorkeur de zorgaanbieders die een aanmeldbericht ontvangen zorgvuldig te selecteren en niet te breed te versturen in het kader van dataminimalisatie en noodzakelijkheid van de verwerking.

3.3.3 Hoe wordt patiënttoestemming vastgelegd?

Zoals eerder beschreven in paragraaf 2.2 is Nuts geen toestemmingsregister. Nuts legt geen toestemmingen vast en logt deze ook niet. Zoals in paragraaf 3.2 beschreven is de zorgaanbieder de verwerkingsverantwoordelijke en heeft deze plicht om de toestemming te kunnen aantonen. De inzet van Nuts verandert niks aan de bestaande situatie.

De wijze van toestemming verlenen en vastleggen is afhankelijk van de zorgtoepassing en de afspraken die door de zorgaanbieders zijn gemaakt daarover. In de specificatie regelen zorgaanbieders en leveranciers hoe ze met (vastlegging van) de toestemming omgaan. Vervolgens kan Nuts die vastgelegde afspraken gebruiken om de grondslagen te valideren voor autorisatie.

Bij een veronderstelde toestemming op basis van een doorverwijzing zoals bij eOverdracht, berust de verwerking van de gegevens alsnog op de grondslag toestemming. Artikel 7 lid 1 AVG vergt van de verwerkingsverantwoordelijke dat hij deze toestemming kan aantonen. Zorgaanbieders doen er dus goed aan om onderling afspraken te maken over de vastlegging van de doorverwijzing in de

[11] https://informatiestandaarden.nictiz.nl/wiki/vpk:V3.1_Opbouw_eOverdracht_aanmelding

eigen bronsystemen. Deze wettelijke plicht staat los van het gebruik van Nuts en geldt ook als partijen geen Nuts gebruiken en gegevens delen op basis van doorverwijzing.

3.4 Babyconnect en Nuts

3.4.1 Beschrijving toepassing Babyconnect

Babyconnect is een versnellingsprogramma (VIPP) dat informatie-uitwisseling in de geboortezorg stimuleert door hierover afspraken te maken in een informatiestandaard. Babyconnect is een vorm van netwerkzorg. Anders dan bij een eenmalige uitwisseling van gegevens zoals bij eOverdracht, vraagt netwerkzorg om een meer continu proces van inzagemogelijkheden, waarbij verschillende zorgaanbieders op verschillende momenten gegevens van elkaar moeten kunnen inzien en gebruiken. Op voorhand is nog niet precies duidelijk, welke zorgaanbieders van het geboortenetwerk de zwangere nodig zal hebben en op welk moment. Voor het programma Babyconnect geldt dat momenteel een pilotfase loopt mbt de inzet van Nuts. Nog niet alles is daarmee al volledig vastgesteld.

Proces Babyconnect via Nuts op hoofdlijnen op basis van de beschrijving in de leveranciersspecificatie van de Toepassing op Nuts Zorginzage 2022:[12]

Babyconnect werkt met generieke toepassingen die sterk lijken op de Nuts Zorginzage 2022. De ontwikkeling is nog niet zover dat Babyconnect een eigen beschrijving van een toepassing op Nuts heeft. De Toepassing Zorginzage 2022 kan drie verschillende typen toestemming ondersteunen, namelijk expliciete specifieke toestemming vooraf aan een afnemer, toestemming op basis van doorverwijzing en de ‘’Wabvpz’’ toestemming.

Het proces van Zorginzage wordt ondersteund met deze Toepassing op Nuts. Dat proces bestaat enerzijds uit het interoperabel, toegankelijk, vindbaar en herbruikbaar (FAIR) maken van dossiergegevens door een bronhouder ('publiceren') en anderzijds uit het daadwerkelijk inzien van dossiergegevens door een afnemer ('raadplegen'). Door Zorginzage zijn zorgverleners in staat het voor hen relevante deel van het zorgtraject van de betrokkene te volgen dat zich bij andere zorgaanbieders afspeelt.

Verschillende zorgaanbieders (eerstelijns verloskundepraktijken, ziekenhuizen, echoscopiepraktijken, kraamzorgorganisaties) moeten in onderlinge samenwerking de juiste zorg voor de betrokkene en diens omgeving leveren. Alle betrokken zorgverleners dienen (wanneer dat voor hen relevant is en wanneer daarvoor een grondslag is) inzage te hebben in de observaties, metingen en andere zorggegevens die zijn geregistreerd door personeel van andere betrokken zorgaanbieders.

Gestandaardiseerde autorisatie van dossiergegevens is een essentieel onderdeel van deze Toepassing op Nuts. Hierbij is het allereerst nodig onderscheid te maken tussen autorisatie-records

[12] https://nuts-foundation.gitbook.io/bolts/zorginzage/zorginzage-2022

enerzijds en grondslagen anderzijds. In de context van deze Toepassing op Nuts is een autorisatie-record een machine leesbaar recht van een zorgaanbieder voor het inzien van een bepaalde scope aan gegevens van een betrokkene. Een autorisatie-record is altijd gebaseerd op een grondslag voor de verwerking van persoonsgegevens. Een bewijs voor een bepaalde grondslag hoeft niet per se machine leesbaar te zijn. In het geval van de grondslag 'toestemming' kan het bewijs bijvoorbeeld bestaan uit een ingescande handtekening of een aangevinkt selectievakje. Er kan echter ook sprake zijn van een mondeling gegeven toestemming. Voor elke zorgtoepassing die gebruik maakt van de Toepassing Zorginzage wordt in het zorgtoepassingsprofiel beschreven welke grondslagen onder welke voorwaarden kunnen worden gebruikt.

In deze Toepassing wordt primair gebruik gemaakt van autorisatie-records die zijn gebaseerd op specifieke toestemmingen.

De Toepassing Zorginzage kan daarnaast ook ondersteuning bieden voor autorisatie op basis van een uitdrukkelijke toestemming voor het vooraf beschikbaar stellen met meerdere niet op voorhand bekende zorgaanbieders (via een elektronisch uitwisselingssysteem) conform de Wabvpz (vanaf hier: 'Wabvpz-toestemming vooraf'). Dit is een door de betrokkene gegeven toestemming aan één specifieke bronhouder of aan alle bronhouders binnen een bepaalde categorie met een behandelovereenkomst met betrokkene, voor het beschikbaar stellen van een afgesproken scope van dossiergegevens van die betrokkene aan een categorie van afnemers met een behandelovereenkomst met betrokkene. Wanneer een Wabvpz-toestemming vooraf wordt voorzien van de juiste cryptografische waarborgen kan deze door een bronhouder, die de Nuts Toepassing Zorginzage heeft geïmplementeerd, worden gebruikt voor het autoriseren tijdens het proces raadplegen.

3.4.2 Is patiënttoestemming vereist?

Zoals uit bovenstaande blijkt kunnen meerdere vormen van toestemming worden ondersteund vanuit de Zorginzage Toepassing op Nuts. Uit gesprekken met het programma Babyconnect is het volgende gebleken als het gaat om de uitwisseling van de medische gegevens in het netwerk: in de huidige situatie is het startpunt van het geboortenetwerk een verloskundige samenwerkingsverband. Dat is een regionaal samenwerkingsverband (VSV) waarin onder meer een ziekenhuis, meerdere verloskundige praktijken en kraambureaus zitten. Hoe groot een VSV precies is, is afhankelijk van de regio. Bij deze meer continue vorm van uitwisseling tussen verschillende zorgaanbieders, is nadrukkelijk toestemming van de patiënt vereist.

Momenteel wordt de toestemming van de patiënt geregeld bij de eerste zorgaanbieder uit het netwerk, de zogenoemde dossierhouderstoestemming. We hebben geen voorbeeld kunnen inzien van deze toestemmingsformulieren echter uit de gesprekken met Babyconnect blijkt dat er wordt uitgegaan van expliciete toestemming vooraf voor gebruik door toekomstige behandelaren.

Door de huidige wijze van inrichting van Babyconnect waarbij de gegevens van de patiënt al van tevoren beschikbaar worden gesteld door de zorgverlener die deze gegevens heeft, zodat een nog onbekende zorgverlener ze kan raadplegen indien noodzakelijk, is sprake van een elektronisch uitwisselingssysteem in de zin van artikel 15a Wabvpz. Als wordt gewerkt met een elektronisch uitwisselingssysteem dat de gegevens al van tevoren beschikbaar stelt, is de benodigde

nadrukkelijke toestemming extra geregeld in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (artikel 15a lid 1 Wabvpz). Als deze toestemming er niet is, is uitwisseling niet mogelijk aangezien de gegevens dan niet in het systeem beschikbaar mogen zijn. Dit betekent dan ook dat er géén uitzonderingen mogelijk zijn, zoals bijvoorbeeld veronderstelde toestemming bij een doorverwijzing. Om vast te stellen of sprake is van een elektronisch uitwisselingssysteem is nader onderzoek nodig mbt de technische werking in de huidige en verwachte situatie, welke data waar worden opgeslagen en wie wanneer toegang heeft tot welke data.

Andere scenario's zijn ook denkbaar. Vanuit Babyconnect worden verschillende scenario's verkend. Een mogelijk groeipad op termijn is een ontwikkeling naar individueel ingerichte zorgnetwerken. Op die manier zou er gezamenlijk met de zwangere kunnen worden bepaald welke zorgaanbieders zij in haar netwerk wil hebben. Dan geeft de zwangere dus per zorgaanbieder specifiek toestemming om deze op te nemen in haar geboortenetwerk zodat gegevens gedeeld kunnen worden. Dan is geen sprake van een elektronisch uitwisselingssysteem.

3.4.3 Hoe wordt patiënttoestemming vastgelegd?

Ook hier geldt dat Nuts geen toestemmingen vastlegt en Nuts logt deze ook niet. Zoals in paragraaf 3.2 beschreven is de zorgaanbieder de verwerkingsverantwoordelijke en heeft deze plicht om de toestemming te kunnen aantonen. De inzet van Nuts verandert niks aan de bestaande situatie.

De zorgaanbieders in het betreffende netwerk moeten dus onderling regelen dat de toestemming die door de eerste zorgaanbieder is verkregen ook beschikbaar is voor de andere zorgaanbieders.

4 Huidige en toekomstige wettelijke vereisten

4.1 AVG

De zorgaanbieders zijn in hun rol als verwerkingsverantwoordelijke, verantwoordelijk voor het voldoen aan de eisen die de AVG stelt. Verwerkingen van persoonsgegevens dienen rechtmatig, behoorlijk en transparant te zijn (artikel 5 lid 1 sub a). Daarnaast mogen gegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verwerkt, dienen de gegevens beperkt te worden tot wat noodzakelijk is voor het betreffende doel en moeten er maatregelen worden genomen om de juistheid van de gegevens te borgen. Gegevens worden niet langer bewaard dan noodzakelijk en er dienen organisatorische en technische maatregelen te worden genomen om ervoor te zorgen dat de gegevens passend zijn beveiligd (artikel 5 lid 1 sub b-f AVG).

Voor het verwerken van bijzondere persoonsgegevens geldt op grond van artikel 9 AVG in beginsel een verwerkingsverbod. Patiëntgegevens zijn bijzondere persoonsgegevens. Verwerking is enkel rechtmatig als aan een van de voorwaarden van artikel 9 lid 2 AVG is voldaan.

4.1.1 Welke persoonsgegevens worden wel via Nuts verwerkt?

In paragraaf 3.2 is toegelicht dat Nuts geen verwerker of verwerkingsverantwoordelijke is, maar een protocol dat door een verwerkingsverantwoordelijk kan worden ingezet als vertrouwenslaag. Uit de stukken blijkt dat de zorgaanbieder via de Nuts node enkel bij de creatie van de autorisatie records van de private claims persoonsgegevens verwerkt indien dit is afgesproken in de specifieke toepassing. Doel hiervan is om de zorgaanbieder te identificeren en om de behandelrelatie tussen een zorgaanbieder en een patiënt vast te stellen. Hierbij wordt in elk geval het BSN van de patiënt verwerkt. Dat is geen bijzonder persoonsgegeven. Wel zijn er strikte regels verbonden aan het verwerken van het BSN. De verwerking van het BSN mag volgens artikel 46 UAVG enkel indien dat bij wet is voorgeschreven ter uitvoering van de doeleinden die bij de wet zijn bepaald.

De wettelijke grondslag voor de zorgaanbieders om het BSN te verwerken staat in hoofdstuk 2 van de Wabvpz. Bij het aangaan van een geneeskundige behandelovereenkomst is de zorgaanbieder verplicht het BSN te registeren (artikel 5 jo. 8 lid 1 Wabvpz). Voor gegevensuitwisseling tussen zorgaanbieders is artikel 9 Wabvpz de grondslag. Volgens artikel 9 Wabvpz vermeldt de zorgaanbieder bij het verstrekken van persoonsgegevens met betrekking tot de verlening van, indicatiestelling voor of verzekering van zorg aan een zorgaanbieder steeds het BSN van de cliënt. De leverancier verwerkt het BSN vervolgens ten behoeve van de zorgaanbieder op basis van deze afgeleide grondslag.

4.1.2 Passende beveiliging van de persoonsgegevens

Artikel 32 AVG schrijft voor dat persoonsgegevens op een passende manier beveiligd moeten worden, gelet op de stand van de techniek, de aard, omvang en context van de doelen die gepaard gaan met de verwerking. Er dienen organisatorische en technische maatregelen te worden genomen om een op het risico afgestemd beveiligingsniveau te garanderen. Aangezien er zowel bijzondere

persoonsgegevens (gezondheidsgegevens) worden verwerkt, dient het beveiligingsniveau daar voldoende op afgestemd te zijn. De verwerkingsverantwoordelijke is hiervoor verantwoordelijk.

Om de gegevens te beschermen zijn technische maatregelen genomen in de Nuts node om de gevoelige data van zorgaanbieders van elkaar te scheiden. De private claims met de autorisatie records zijn per zorgaanbieder of per zorgteam in een afgescheiden cryptografisch versleutelde wallet opgenomen waar enkel toegang kan worden verkregen met een technische identifier (DID). Op deze manier worden het BSN en de gegevens die mogelijk herleidbaar zijn tot een individu werkzaam bij de zorgaanbieder geïsoleerd conform NEN-7510. Deze private claims worden niet gesynchroniseerd over alle Nodes van het Nuts netwerk. De private claims komen enkel terecht in de wallets van de twee zorgaanbieders die een uitwisseling tot stand (willen) brengen.

Het beoordelen of voldaan wordt aan het instellen van passende technische en organisatorische maatregelen voert te ver voor dit onderzoek en zal, indien nog niet beoordeeld, door de verwerkingsverantwoordelijke moeten worden vastgesteld.

4.2 WGBO

De algemene rechten van de patiënt zijn neergelegd in de Wet op de geneeskundig behandelingsovereenkomst (WGBO). De WGBO is als bijzondere overeenkomst in het Burgerlijk Wetboek (BW) opgenomen in afdeling 5 van boek 7: artikel 446 en volgende. Ten aanzien van het uitwisselen van gegevens zijn de volgende patiëntenrechten relevant voor deze analyse:

1) art. 7:454 BW: de dossierplicht voor de zorgverlener
2) art. 7:455 BW: het vernietigingsrecht voor de patiënt.
3) art. 7:456 BW: recht op inzage en afschrift van het dossier in de zin van art. 7:454 BW
4) art. 7:457 BW: recht op het medisch beroepsgeheim. De hoofdregel is dat er toestemming vereist is om het medisch beroepsgeheim te doorbreken (lid 1). Als uitzonderingen op deze hoofdregel noemt de WGBO : een wettelijke plicht of taak, rechtstreeks bij de behandeling betrokken en uitwisseling met een vervanger of waarnemer van de zorgverlener.
5) art. 7:458 BW: regelt onder welke voorwaarden bij medisch-wetenschappelijk onderzoek een uitzondering kan worden gemaakt op het toestemmingsvereiste.

4.3 De Wabvpz

De Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) omvat waarborgen voor cliënten bij elektronische gegevensuitwisseling. Een deel van de wettelijke bepalingen is per 1 juli 2017 in werking getreden. De bepalingen rondom kosteloze elektronisch afschrift/inzage en logging zijn per 1 juli 2020 in werking getreden (artikel 15d). De Wabvpz ziet zowel op dossiers van de zorgaanbieder als elektronische uitwisselingssystemen. Met een elektronisch uitwisselingssysteem wordt bedoeld: “een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, waaronder niet begrepen een systeem binnen een zorgaanbieder, voor het bijhouden van een elektronisch dossier”. Voorbeelden hiervan zijn inzageportalen en systemen met verwijsindexen, zoals het Landelijk Schakelpunt (LSP). Indien de medische gegevens beschikbaar worden gesteld via een elektronisch uitwisselingssysteem dan is de

zorgaanbieder verplicht om uitdrukkelijke toestemming aan de cliënt te vragen (artikel 15a). De Wabvpz bevat ook BSN-wetgeving voor de zorg (verplicht gebruik BSN voor zorgverleners, zorgverzekeraars en indicatieorganen).

Bij de Wabvpz hoort bovendien het 'Besluit elektronische gegevensuitwisseling zorgaanbieders'. Via dit besluit zijn de NEN 7510:2017 (informatiebeveiliging); de NEN 7512 en de NEN 7513 (logging) verplicht gesteld.

4.4 De Wegiz

De Wet elektronische gegevensuitwisseling in de zorg (Wegiz) bevat een aantal algemene uitgangspunten. Ten eerste maakt de Wegiz het mogelijk om gegevensuitwisselingen tussen zorgaanbieders aan te wijzen die voortaan verplicht elektronisch moeten verlopen. Ten tweede verplicht de Wegiz zorgaanbieders niet welke gegevens moeten worden uitgewisseld. Dat moet het zorgveld zelf bepalen aan de hand van de noodzaak om goede zorg te kunnen verlenen. Twee andere belangrijke uitgangspunten van de Wegiz zijn eenheid van taal en eenheid van techniek.

Zodra de gegevensuitwisseling geselecteerd wordt om verplicht elektronisch te verlopen dienen zorgaanbieders en ICT-leveranciers afspraken met elkaar te maken over de uitwisseling op het gebied van taal, techniek en ICT. Deze informatiestandaarden worden neergelegd in NEN-normen.

De Verpleegkundige Overdracht staat bijvoorbeeld op de meerjarenagenda van de Wegiz. Daarvoor is recent een werkgroep ingesteld die de informatiestandaard NEN 7545 onder de Wegiz aan het ontwikkelen is.

Bij de behandeling van de Wegiz in de Tweede Kamer is een motie aangenomen die voorstelt om op wettelijk niveau de verplichting op te nemen dat elke elektronische gegevensuitwisseling van medische gegevens end-to-end beveiligd is, wat zowel end-to-end authenticatie en end-to-end encryptie omvat. In een Kamerbrief[13] van 15 december 2022 heeft De Minister aangegeven dat NEN-normen op dit gebied onverkort gelden en dat het direct verplicht stellen van end-to-end encryptie mogelijk leidt tot een vertraging van het tempo waarmee de gegevensuitwisseling in de zorg kan worden doorgevoerd. De Minister wil nader onderzoek laten doen naar de technische en organisatorische vraagstukken die een dergelijke verplichting oplevert en welke kosten daaraan verbonden zijn. Pas na de resultaten van dit onderzoek zal worden bezien of, en zo ja, hoe end-to-end versleuteling en authenticatie verplicht kunnen worden onder de Wegiz. Voor Nuts is dit in de toekomst mogelijk een aandachtspunt, hoewel er geen medische gegevens via Nuts lopen.

De Tweede Kamer heeft het wetsvoorstel in september 2022 unaniem aangenomen. Het wetsvoorstel wordt momenteel schriftelijk in de Eerste Kamer voorbereid. De plenaire behandeling staat gepland op 11 april en de stemming zal waarschijnlijk plaatsvinden op 18 april 2023.

[13] Kamerstukken II 2021/22, 27529, nr. 288.

4.5 De EHDS

De Europese Commissie heeft op 3 mei 2022 de conceptverordening 'Europese ruimte voor Gezondheidsgegevens' (European Health Data Space – EHDS) gepubliceerd. De EHDS-verordening biedt een kader voor het elektronisch verwerken van gezondheidsgegevens voor drie doelen: het primair gebruik van zorgdata, het secundair gebruik van zorgdata en de ontwikkeling van een interne markt voor digitale gezondheidsproducten en -diensten, zoals EPD's en gezondheidsapps. Bovendien bevat de EHDS bepalingen over de governance van data, zowel voor primair als secundair gebruik. Wat betreft primair gebruik gaat het daarbij grotendeels om dezelfde geprioriteerde gegevensuitwisselingen als bij de Wegiz. De meeste discussie over de EHDS vindt plaats over het secundair (hergebruik) van elektronische gezondheidsgegevens. Nuts is niet alleen toe te passen voor primair gebruik, maar ook voor secundair gebruik. Bij KiK-V (Keteninformatie Kwaliteit Verpleeghuiszorg) is Nuts al toegepast voor secundair gebruik.

Op dit moment wordt nog door de lidstaten onderhandeld over het voorstel voor de EHDS. In de zomer vindt de behandeling van het voorstel plaats in het Europees Parlement.

4.6 De Wdo - toekomst UZI

De Wdo wordt in verschillende tranches ingevoerd. De Eerste Kamer heeft op 21 maart de Wet digitale overheid (Wdo) aangenomen. Daarmee eindigt de parlementaire behandeling van dit wetsvoorstel. Na ondertekening door de Koning en de Minister van BZK zal de wet gepubliceerd worden in het Staatsblad. Met deze wet wordt een belangrijke stap gezet op het gebied van veilige digitale toegang die ook impact heeft op de zorgsector. Het doel van het wetsvoorstel Wet Digitale Overheid is om ervoor zorgen dat burgers veilig en betrouwbaar kunnen inloggen bij alle (semi)-overheden met een geaccepteerd inlogmiddel naar keuze. Inloggen moet mogelijk zijn met elk identificatiemiddel (eID) die een substantiële of hoge betrouwbaarheid kan bieden. De toe te laten middelen moeten voldoen aan de eIDAS-verordening.

(Semi)-publieke dienstverleners worden verplicht om een passend beveiligingsniveau van hun diensten te kunnen verzekeren en identificatiemiddelen met niveau substantieel of hoog te accepteren om burgers toegang te geven tot hun diensten met identificatiemiddelen die hieraan voldoen. Zorgaanbieders zijn door de Wdo aangemerkt als dienstverleners die onder de scope van de wet vallen. Dit is vermeld in onderdeel 3 in de bijlage van de wet.

De Wdo regelt nu enkel nog de situatie dat een burger of bedrijf wil inloggen op een digitale omgeving van een zorgaanbieder, en niet de situatie waarin digitale transacties tussen zorgaanbieders onderling plaatsvinden. De Wdo is een kaderwet met een flexibel karakter. Op die manier kan er ingespeeld worden op nieuwe ontwikkelingen. Het is daardoor goed mogelijk dat de Wdo in de toekomst ook het betrouwbaar inloggen tussen semi-publieke instellingen onderling zal gaan regelen, met een vergelijkbare acceptatieplicht van identificatiemiddelen.

Programmateam Toekomstbestendig maken UZI-middelen– ministerie van VWS
Voor het toekomstbestendig maken van identificatie en authenticatie van professionals in de zorg is er een flexibel stelsel met verschillende betrouwbare inlogmiddelen op komst. De verwachting is dat de nieuwe inlogmiddelen niet alleen beter passen in verschillende zorgprocessen en op veel plekken

te gebruiken zijn, ze kunnen ook door meer zorgprofessionals gebruikt worden. Uit gesprekken met het programmateam Toekomstbestendig maken UZI komt naar voren dat het beleid voor de toekomst is dat in de zorg door professionals gebruik gemaakt kan worden van alle identificatiemiddelen die straks onder de Wdo geaccepteerd worden, daarnaast zal een vorm van certificering worden ontwikkeld waarbij ook middelen voor zorgprofessionals van grote zorgaanbieders die voldoen aan de eisen worden geaccepteerd. Vooralsnog is nog geen sprake van een verplichting als het gaat om zorgprofessionals. Het is daarom raadzaam voor Nuts om in dit kader de nodige voorbereidingen te treffen zodat de implementatie van Nuts niet in de weg staat aan de acceptatie daarvan. Nuts schrijft in de basis geen specifiek identificatiemiddel voor, enkel dat het middel op cryptografische wijze aan validatie doet. Vanuit Nuts wordt ook aangegeven dat rekening wordt gehouden met deze ontwikkeling en meerdere middelen geaccepteerd zullen kunnen worden - naast IRMA - en nu nog de UZI-pas. Voor de UZI-pas geldt dat de (huidige) planning is dat deze in 2028 uitgefaseerd wordt en de nieuwe situatie gaat gelden.

4.7 eIDAS

eIDAS staat voor ‘Electronic Identities And Trust Services’. Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. Dit kan alleen met een betrouwbare online identiteitscheck aan de voordeur.

Nederlandse overheidsorganisaties en private organisaties met een publieke taak moeten sinds 29 september 2018 Europees erkende inlogmiddelen accepteren in hun digitale dienstverlening. De lidstaten van de EU hebben dit met elkaar afgesproken in de eIDAS-verordening. Hierdoor wordt het makkelijker en veiliger om binnen Europa online zaken te regelen.

eIDAS onderscheidt drie betrouwbaarheidsniveaus: laag, substantieel en hoog. Gezondheidsgegevens die onder het medisch beroepsgeheim vallen behoren tot betrouwbaarheidsniveau hoog.

5 Blockchain en cryptografie

5.1 Blockchain en Nuts

Ui de gesprekken met de vertegenwoordigers van Nuts komt naar voren dat Nuts geen gebruik maakt van blockchain technologie, omdat blockchain technologie te 'zwaar' is voor Nuts. Blockchains ondersteunen in de kern consensus binnen een netwerk. In Nuts publiceren partijen alleen hun eigen publieke gegevens in het netwerk en is consensus niet nodig. Mogelijk is het idee ontstaan dat Nuts blockchain gebruikt, omdat bepaalde technische fenomenen zoals ''nodes'', ''cryptografie'' ''hashing'' en ''decentraal en een gedistribueerd netwerk'' zowel een rol spelen bij blockchain technologie als bij Nuts. Hieronder wordt uitgelegd wat blockchain technologie in algemene zin is en waarom de techniek niet bij de visie van Nuts past.

Blockchain is een systeem voor het opslaan van gegevens in een aaneengeschakelde keten van datablokken waarbij deze blokken niet gewijzigd kunnen worden. Elk blok dat nieuw aan de keten worden toegevoegd, verwijst naar het voorgaande blok door middel van een hash, waardoor het eenvoudig te controleren is of de opvolgende blokken ook daadwerkelijk gerelateerd zijn aan elkaar. Controle gebeurt op basis van een decentraal netwerk van nodes, die vaststellen of de hash klopt en of deze de juiste elektronische handtekening(en) bevat. Alle nodes hebben een identieke kopie van dit ''grootboek'' en kunnen elkaar op die manier controleren. Zo ontstaat er consensus over de juistheid van de blokken zodat deze integer, onweerlegbaar en onveranderlijk worden. Deze functionaliteit van blockchains wordt ook door de Nuts nodes geboden om zo de adresgegevens van de technical endpoints van de op het Nuts netwerk aangesloten systemen van (de leveranciers van) zorgaanbieders te kunnen delen en vinden.[14]

Blockchain verschilt van Nuts in het belang dat Blockchain hecht aan consensus in het netwerk over elke transactie en interactie. Omdat dit in blockchains veelal financiële waarden of -transacties vertegenwoordigt, is de hoeveelheid energie die besteed moet worden door (deelnemers in) het netwerk om bewijs van de integriteit van data te leveren heel hoog. In Nuts is dit niet nodig omdat de (leverancier van) de zorgaanbieder de eigen informatie publiceert en digitaal ondertekent.

Een nadeel van blockchain is dus dat de decentralisatie van het netwerk waar die gepaard gaat met de behoefte aan consensus veel 'werk' (en dus potentieel veel kosten) oplevert voor de nodes in de blockchain. De gegevens die door de Nuts nodes gepubliceerd worden (de technische adressen van de endpoints van de zorgaanbieders) vallen steeds onder verantwoordelijkheid van één zorgaanbieder en behoeven geen consensus. Daarom is blockchain zowel functioneel als qua kosten geen goede fit voor Nuts.

Gezien Nuts geen gebruik maakt van blockchain technologie en daarvan voor zover te voorzien valt ook geen gebruik wil gaan maken in de toekomst, is de vraag irrelevant, in hoeverre blockchain nadere eisen met zich mee brengt ten aanzien van het gebruik van gegevens in de verpleegkundige overdracht.

[14] RFC004 Verifiable Transactional Graph - V1 (gitbook.io)

5.2 Cryptografische toepassingen binnen Nuts

Nuts maakt gebruik van cryptografische technieken. Gedurende de gehele gegevensverwerking via Nuts blijven de gegevens versleuteld. Het vertrouwensmodel van Nuts (identiteit, authenticatie en logging) is geheel vastgelegd in cryptografie. De hele vertrouwenslaag die Nuts is, is gebaseerd op de cryptografische principes van "ondertekenen", waarmee een stukje informatie in het netwerk altijd te koppelen is aan de oorspronkelijke auteur. Dit maakt het mogelijk een decentraal netwerk op te zetten, waarbij alle informatie (gebaseerd op de governance van dat stuk informatie) te vertrouwen is.

Nuts lijkt op Multi Party Computation (MPC), cryptografische technieken om gezamenlijke berekeningen mogelijk te maken op beschermde data zonder participanten toegang te geven om te lezen of te bewerken. MPC verwerkt governanceregels in cryptografie.
Nuts lijkt ook op de Personal Health Train (PHT), in plaats van alle data uit verschillende bronnen te verzamelen, brengt de PHT de analyse naar de verschillende databronnen. Deze toepassing is niet verder beschreven in bovenstaande analyse maar vorig jaar is bij het programma KiK-V (Keteninformatie Kwaliteit Verpleeghuiszorg) een beproeving gedaan met Nuts en PHT.

6 Governance

6.1 Algemene governance van het Nuts netwerk

De governance van Nuts werkt overeenkomstig de governance van internet-protocollen, vergelijkbaar met het GSM-protocol. Nuts hanteert een decentrale manier van denken over governance en toezicht. Het vertrouwensmodel werkt en op basis van cryptografie. Hierop laat Nuts audits doen.

In feite biedt Nuts een Public Key Infrastructure (PKI) zonder centrale autoriteiten en is daardoor goed schaalbaar. Iedereen heeft persoonlijke sleutels en publieke sleutels. De public key deel je en gebruik je om met elkaar te communiceren. Alles wat je doet in het netwerk kan je ondertekenen met je private key en is aantoonbaar/herleidbaar naar jou.

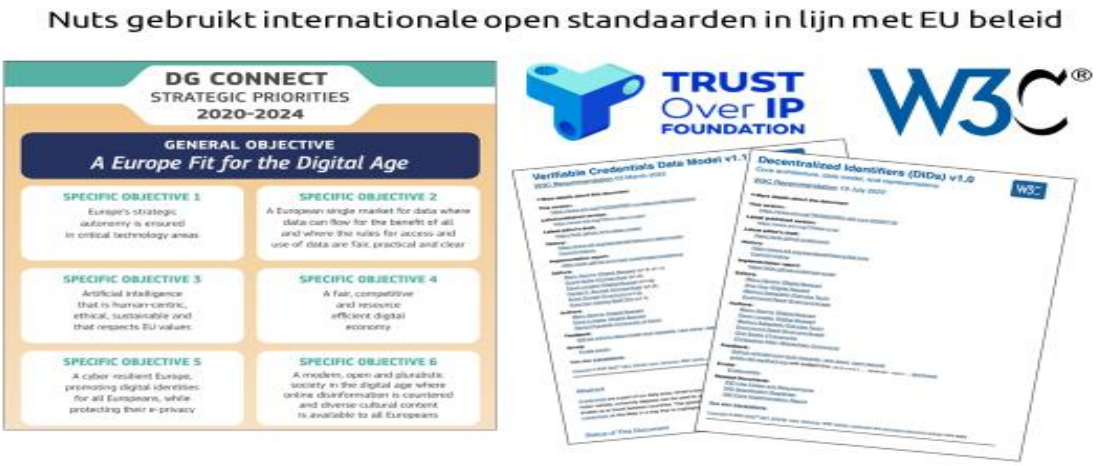
Pas na ondertekening van de aansluitovereenkomst kunnen partijen op het Nuts netwerk.

Per specifieke toepassing is er een toepassingsoverleg, Als daar iets wordt gevraagd dat binnen Nuts niet past, dan wordt dit voorgelegd aan het toepassingsoverstijgend overleg.

Naast de governance van het Nuts netwerk zijn er in de Nuts community nog andere relevante governance-uitwerkingen. Ten eerste in het Nuts Manifest (https://nuts.nl/manifest/), waarin de overtuiging dat medische data aan de patiënt en de zorgprofessional toebehoort vorm krijgt via data protection by design, security by design en cryptografie. Ten tweede de wijze waarop de interne besluitvorming is ingericht als waardenetwerk van iedereen voor iedereen, waarvoor ieders toestemming noodzakelijk is. Ten derde de wijze waarop de Nuts node de Nuts open standaarden implementeert in de vorm van een Open Source applicatie waarmee samen decentraal een federatief netwerk wordt vormgegeven.

6.2 Internationale governance-aspecten Nuts: gebruik van internationale open standaarden

In onderstaande figuur blijkt dat Nuts in haar ontwerp en mogelijkheden de Nederlandse Zorg-ICT overstijgt. Nuts maakt gebruik van internationale open standaarden, Verifiable Credentials en Decentralized Identifiers en ontwikkelt haar governance door aan de hand van het internationale TrustOverIP vertrouwensmodel. Aan dit model werkt een wereldwijd consortium van partijen samen om vertrouwen op de schaal van het internet te realiseren.



6.3 Communicatie, toezicht en verantwoording

Communicatie over hoe de governance van Nuts onder de motorkap werkt is een uitdaging omdat het een nieuw paradigma is. Aangetoond moet kunnen worden dat Nuts inderdaad veilig is en voldoet aan de standaarden. Dat vergt een goede communicatiestrategie. Onder andere door het wegnemen van de vele misverstanden die voorafgaand in deze rapportage al aan de orde kwamen.

Men denkt bij de governance al snel aan de governance van een gehele toepassing, inclusief de bijbehorende infrastructuur, zoals eOverdracht en Babyconnect. Daar zitten heel veel afspraken in op het niveau van de zorgaanbieder of het niveau van de leverancier. Als je het afpelt tot de governance van Nuts, dan blijft er enkel techniek en administratie over. In principe controleert Nuts technisch en administratief of de partij daadwerkelijk een zorgaanbieder is. De governance zit op het niveau van de toepassing in plaats van in de infrastructuur.

Stel dat één van de Nodes gecompromitteerd wordt door hackers, dan wordt dit opgelost via de open source community, waarin de lijntjes kort zijn en men elkaar snel helpt. De Nuts node hoort bij de partij die dit in zijn systeem bouwt. Die node is dus niet eigendom ‘’van Nuts’’. Per applicatie is er een Nuts node. Als een Nuts node in het netwerk wordt gecompromitteerd dan valt deze uit. Dankzij het decentrale netwerk blijft de rest van de nodes intact. Het netwerk kan gewoon doorgaan. Zelfs als een deel van het netwerk eruit zou liggen, zou het andere deel nog kunnen blijven draaien, vergelijkbaar met het internet.

In de aansluitovereenkomst is opgenomen dat er afspraken aanwezig moeten zijn over het hebben van een beheer- en supportorganisatie. Uiteindelijk is het aan zorgaanbieders zelf om dit te regelen in de SLA. Als de node in de praktijk niet goed wordt onderhouden, zal de node uitvallen.

In de aansluitovereenkomst wordt verondersteld dat de zorgaanbieders zelf enige expertise hebben om een goede IT-leverancier te kiezen. Dit is een uitdaging en aandachtspunt voor de toekomst en kan best moeilijk zijn voor kleinere zorgaanbieders. Aan de andere kant is een decentraal netwerk veel robuuster en betrouwbaarder doordat het open source is. Iedereen kan immers meedenken om het te verbeteren. Wellicht is het goed om een raamwerk voor kleinere aanbieders te ontwikkelen.

Tot besluit is het juridisch en qua governance van belang dat over het netwerk van Nuts geen patiëntgegevens worden uitgewisseld. Dat scheelt veel juridische vereisten waarop anders toezicht gehouden zou dienen te worden. Nuts zorgt er voor dat infrastructuur en data los van elkaar zijn gekoppeld.

7 Conclusies

- De Nuts community is een open source software ecosysteem dat een open protocol maakt en publiceert dat het mogelijk maakt voor computers om met elkaar te kunnen communiceren zoals het Internet Protocol (IP). Waar het internet ons in staat stelt anoniem met anderen te communiceren, zorgt Nuts er voor dat de communicatie via internet niet langer anoniem is door een vertrouwenslaag aan het netwerk toe te voegen.
- Het blijkt dat het in de praktijk vaak nog lastig is om te begrijpen wat Nuts nu echt is. Met regelmaat wordt bijvoorbeeld gedacht dat Nuts een toestemmingsvoorziening is die concurreert met Mitz. Nuts registreert geen toestemmingen en uit de analyse komt naar voren dat Nuts juist op termijn zou kunnen werken met toestemmingen die zijn geregistreerd in Mitz. Een ander misverstand is dat de patiëntgegevens uit het medische dossier ook via Nuts worden verstuurd. Dit is niet het geval, de daadwerkelijke uitwisseling van de patiëntgegevens vindt plaats via andere systemen van de zorgaanbieders.
- Van belang is dat op een heldere wijze wordt gecommuniceerd over wat Nuts wel en niet is, met name voor doelgroepen zonder uitgebreide technische kennis zoals beleidsmakers, bestuurders en juristen.
- Als het gaat om of patiënttoestemming is vereist en zo ja in welke vorm dan is dit afhankelijk van de specifieke toepassing. Zoals uit de geanalyseerde toepassingen blijkt kan dit verschillen en moet dit door de zorgaanbieders worden vastgesteld en afgesproken. Bijvoorbeeld bij eOverdracht is sprake van een doorverwijzing en daarmee kan gebruik worden gemaakt van veronderstelde toestemming. Bij Babyconnect lijkt het in de huidige vorm zo te zijn dat sprake is van een elektronisch uitwisselingssysteem in de zin van artikel 15a Wabvpz. Als wordt gewerkt met een elektronisch uitwisselingssysteem dat de gegevens al van tevoren beschikbaar stelt, is de benodigde nadrukkelijke toestemming extra geregeld in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (artikel 15a lid 1 Wabvpz).
- Patiënttoestemming wordt niet vastgelegd in Nuts maar moet, net zoals in de huidige situatie, door de zorgaanbieder worden geregistreerd zodat men kan voldoen aan de aantoonplicht onder de AVG die geldt voor een verwerkingsverantwoordelijke die de grondslag toestemming gebruikt voor een verwerking.
- Als het gaat om de huidige wet- en regelgeving dan is een belangrijke conclusie dat deze met name van toepassing is op de zorgaanbieder. De zorgaanbieder moet voldoen aan de wettelijke vereisten vanuit de AVG, Wgbo, Wabvpz en eIDAS en moet daarmee ook zorgen dat de door hen gekozen toepassingen en software voldoen aan de gestelde eisen. Dit staat los van het gebruik van Nuts maar geldt voor alle systemen die door de zorgaanbieder worden gebruikt. Er is een aantal ontwikkelingen van invloed op de toekomstige wettelijke vereisten zoals de Wegiz, EHDS, Wdo en Toekomst UZI.
- Nuts maakt geen gebruik van Blockchain en hier is ook geen noodzaak toe. De reden dat er niet voor blockchain is gekozen, is dat bij Nuts geen consensus nodig is. Partijen publiceren alleen hun eigen publieke gegevens in het netwerk, er is dus geen sprake van potentieel conflicterende transacties en er hoeft dus ook niet tot consensus te worden gekomen.
- Nuts maakt gebruik van cryptografische technieken. Gedurende de gehele gegevensverwerking via Nuts blijven de gegevens versleuteld. Het vertrouwensmodel van

Nuts (identiteit, authenticatie en logging) is geheel vastgelegd in cryptografie. De hele vertrouwenslaag die Nuts is, is gebaseerd op de cryptografische principes van "ondertekenen", waarmee een stukje informatie in het netwerk altijd te koppelen is aan de oorspronkelijke auteur. Dit maakt het mogelijk een decentraal netwerk op te zetten, waarbij alle informatie (gebaseerd op de governance van dat stuk informatie) te vertrouwen is. Uiteraard heeft binnen deze opdracht geen technische audit plaatsgevonden van de cryptografische technieken. Indien behoefte bestaat in inzicht daarin zal dit apart moeten worden onderzocht.

- De governance van het Nuts netwerk is vergelijkbaar met de governance van het GSM-protocol. Nuts maakt gebruik van internationale open standaarden, Verifiable Credentials en Decentralized Identifiers en ontwikkelt haar governance door aan de hand van het internationale TrustOverIP vertrouwensmodel. Het kent daarmee geen centrale governance en toezicht zoals bij ICT-infrastructuur in de zorg gebruikelijker is. Het voordeel is dat er geen sprake is van ‘one point of failure.’ Een nadeel is dat het lastiger te begrijpen is. Nuts lost dit door een vertrouwensmodel op basis van cryptografie en laat hier audits op doen en is steeds transparant over hoe hun model in elkaar zit.

Parkstraat 20, 2514 JK Den Haag **T** +31(0)6 39278533 **E** info@hooghiemstra-en-partners.nl
ING Bank NL49INGB0008938076 **www**.hooghiemstra-en-partners.nl **KvK** 73390356 **BTW** 8595.06.447.B01