Reactie op consultatie – Wet Diaz
12 augustus 2023, opgesteld door Twiin (www.twiin.nl)

Doel van de wet zoals Twiin dat begrijpt – betrouwbare inlog bij SBV-Z

Met dit consultatiewetsvoorstel wordt o.a. mogelijk gemaakt dat zorgaanbieders en zorgmedewerkers gebruik kunnen maken van inlogmiddelen op het hoogste betrouwbaarheidsniveau voor het raadplegen van SBV-Z om het BSN van cliënten te verifiëren en om het gebruik deze middelen voor gegevensuitwisseling mogelijk te maken. Het wetsvoorstel biedt ruimte voor het gebruik van verschillende inlogmiddelen:

1. Op basis van de Wdo erkende publieke en private inlogmiddelen;
2. Zorgspecifieke inlogmiddelen; en
3. PKI-o-middelen.

De zorgspecifieke inlogmiddelen moeten gecertificeerd zijn op basis van NEN7518 om er gebruik van te mogen maken voor het raadplegen van SBV-Z om het BSN van cliënten te verifiëren.

Met dit consultatiewetsvoorstel kunnen zorgmedewerkers zich laagdrempelig inschrijven in het UZI-register. Met zorgmedewerker wordt eenieder bedoeld die werkzaam is of wil zijn in de zorg.

Reactie Twiin op algemeen doel van de wet

Het is positief dat met dit consultatiewetsvoorstel ook niet BIG-geregistreerde zorgmedewerkers zich kunnen inschrijven, zodat ook zij de BSN-controle kunnen uitvoeren. Het is immers vaak een administratief medewerker die dit soort controles uitvoert.

Het is positief dat het consultatiewetsvoorstel ruimte biedt aan zorgspecifieke middelen, zoals een ziekenhuispas, aangezien die goed aansluiten bij bestaande zorgprocessen.

Uit de toelichting bij het consultatiewetsvoorstel volgt dat voor zorgaanbieders een koppeling met een HR-systeem mogelijk wordt gemaakt om te zorgen voor geautomatiseerd aanmelden in het register. Dat roept vragen op over de eisen die gesteld zullen worden aan de beveiliging van zo'n HR-systeem. Wenselijk is dat eisen worden gesteld aan zo'n systeem voordat koppeling mogelijk is. Gedacht kan worden aan NEN7510 certificering met een verklaring van toepasselijkheid die ruim genoeg is om ook betrekking te hebben op dit HR-systeem.

Hoe Twiin begrijpt dat de wet identificatie bij gebruik elektronisch uitwisselingssysteem regelt

De certificering van zorgspecifieke inlogmiddelen is op basis van dit consultatiewetsvoorstel niet verplicht als het gaat om uitwisseling van gegevens op basis van de Wegiz. Ook regelt dit consultatiewetsvoorstel geen verplichting om gebruik te maken van de erkende inlogmiddelen en het UZI-register voor toegang tot uitwisselings- en/of zorginformatiesystemen ten behoeve van elektronische gegevensuitwisseling in de zorg. Het is aan zorgaanbieders om zelf te bepalen of zij de nieuwe inlogmiddelen willen gebruiken voor eigen elektronische uitwisselingssystemen.

Als een zorgaanbieder eenmaal beschikt over een gecertificeerd zorgspecifiek inlogmiddel, is waarschijnlijk dat de zorgaanbieder deze ook zal willen gebruiken voor inloggen in een uitwisselings- en/of zorginformatiesysteem. Dat roept de vraag op of de eisen die de wet stelt aan de certificering ook afdoende zijn voor gebruik bij een uitwisselings- en/of zorginformatiesysteem. Dat zal mede afhankelijk zijn van de NEN7518 norm waarin wordt vastgelegd aan welke eisen die inlogmiddelen moeten voldoen.

De toelichting bij het wetsvoorstel noemt dat de NEN7518 norm eisen zal stellen aan de zorgspecifieke middelen, zoals eisen met betrekking tot de identificatie van de zorgmedewerker, het registratie- en beheerproces van deze (digitale) identiteit en de uitgifte van het zorgspecifieke middel aan een zorgmedewerker.

Reactie Twiin ontbreken verplichting gebruik elektronisch uitwisselingssysteem

Om het vertrouwen bij het beschikbaar stellen en uitwisselen van gegevens in de zorg te borgen, is het gebruik van betrouwbare inlogmiddelen noodzakelijk. Dit wetsvoorstel bevordert het gebruik van inlogmiddelen met hoog betrouwbaarheidsniveau voor toegang tot uitwisselings- en/of zorginformatiesystemen. Dat is positief.

Maar het wetsvoorstel verplicht niet tot het gebruik van middelen die op basis van NEN7518 gecertificeerd zijn en/of WDO-middelen voor toegang tot uitwisselings- en/of zorginformatiesystemen. Dat roept vragen op. Immers volgt al uit de toepasselijke beveiligingsnormen voor de zorg dat gebruik van inlogmiddelen met betrouwbaarheidsniveau hoog verplicht zijn als het gaat om toegang tot gegevensuitwisseling. Dit volgt uit de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening. Een wettelijke verplichting tot het gebruik van middelen die op basis van NEN7518 gecertificeerd zijn en/of WDO-middelen voor toegang tot uitwisselings- en/of zorginformatiesystemen lijkt daar goed bij aan te sluiten.

Het doel van de wet is kortom te smal. Voor de *verwerking* van privacygevoelige gegevens van bijzondere aard (zoals medische gegevens) past een authenticatiemiddel van het hoogste betrouwbaarheidsniveau. Dat gaat niet alleen over het uitwisselen van medische gegevens, maar over het überhaupt toegang krijgen tot medische gegevens, ook lokaal. Het wetsvoorstel is nu ingestoken dat voor twee scenario's waarin gegevens met een andere partij uitgewisseld worden (SBV-Z en andere zorgaanbieder) een *ander* authenticatiemiddel vereist zou worden dan voor het ‘dagelijkse gebruik’ in het lokale EPD. Dit draagt niet bij aan de acceptatie van deze middelen/de manier van werken. Het voorstel zou daarom zijn dat

het wetsvoorstel primair regelt dat er authenticatiemiddelen op het hoogste betrouwbaarheidsniveau beschikbaar komen voor toegang tot medische gegevens in zijn algemeenheid waardoor de in het wetsvoorstel nu genoemde situaties daar automatisch onder vallen. Dit moet dan in artikel 14 komen.
Op deze manier is er voor zorgaanbieders alleen nog een keuze voor een middel dat aan de NEN7518 voldoet zodat vervolgens de medewerkers al hun werk daarmee kunnen uitvoeren.

Wel is positief dat eisen worden gesteld aan die zorgspecifieke middelen, zoals eisen met betrekking tot de identificatie van de zorgmedewerker, het registratie- en beheerproces van deze (digitale) identiteit en de uitgifte van het zorgspecifieke middel aan een zorgmedewerker. Of deze eisen voldoende zijn voor een betrouwbare inlog, is overigens de vraag. Immers is meer nodig dan enkel een persoonlijke inlog, waaronder gebruik van identificatiemiddelen die de toepassing van een autorisatieprotocol mogelijk maken.

Overigens zorgt de plicht om te certificeren op basis van NEN7518 mogelijk voor een extra administratieve last bij de zorgaanbieder, tenzij de zorgaanbieder gebruik kan maken van WDO-middelen. Wenselijk is om te borgen dat die certificering zo goed mogelijk aansluit bij de NEN7510 certificering. Zeker nu NEN7510 ook al bepaalt dat de zorgaanbieder een procedure moet inrichten voor het toewijzen en intrekken van toegangsrechten en daarbij eisen stelt aan het beheer van toegangsrechten en het gebruik ervan.

Overigens is wel de vraag hoe zinvol en toekomstbestendig het is om NEN7518 middelen te mogen gebruiken naast WDO-middelen. Academische ziekenhuizen zijn op basis van eIDAS sowieso al verplicht om WDO-middelen te gebruiken. Bij uitwisseling van medische gegevens over landsgrenzen heen – in de toekomst verplicht op basis van de EHDS – zal het gebruik van WDO-middelen wellicht ook nodig blijken. NEN7518 is immers een Nederlandse norm en lijkt daarmee niet geschikt voor vertrouwen over landsgrenzen heen. Dat roept de vraag op of het mogelijk zal zijn om NEN7518 middelen ook te laten kwalificeren als WDO-middelen. En zo ja, dan is de vraag wat de toegevoegde waarde is van een NEN7518 certificering naast een toelating als WDO-middel.

Reactie Twiin algemene eisen aan inlogmiddelen

Om de gegevensuitwisseling in de zorg te bevorderen, is standaardisering gewenst. Gegevensuitwisseling in de zorg is er mee gebaat dat de identiteit is gekoppeld aan een gestandaardiseerde omschrijving van de rol van degene die geïdentificeerd wordt.

De toelichting schrijft dat het wetsvoorstel door middel van de persoonlijke inlog zal borgen dat enkel diegenen die hiertoe gerechtigd zijn clientgegevens kunnen raadplegen.

Om te borgen dat enkel diegenen die hiertoe gerechtigd zijn clientgegevens kunnen raadplegen, is echter meer nodig dan een persoonlijke inlog. Ook is bijvoorbeeld nodig dat een autorisatiebeleid wordt ingericht en toegepast. En voor een autorisatiebeleid is het

nodig om te controleren aan welke zorgaanbieder een zorgmedewerker is verbonden. Ook is nodig om na te gaan welke rol een zorgmedewerker heeft.

In het consultatiewetsvoorstel is geen duidelijke koppeling voorgeschreven tussen de zorgverlener en de zorgaanbieder. Zo'n koppeling lijkt wel verstandig, mede omdat een zorgverlener voor meerdere zorgaanbieders kan werken. Voor een goede autorisatie is het nodig dat de identiteit van de zorgverlener gekoppeld kan worden aan de juiste identiteit van de zorgaanbieder.

Onduidelijk is verder of het register dat wordt ingericht gekoppeld zal worden aan het register voor zorgaanbieders dat al is ingericht op basis van de Wtza. Wenselijk lijkt om de registratie van zorgaanbieders in een register op slechts één plek uit te voeren. In dat geval is verduidelijking nodig of enkel zorgaanbieders die beschikken over een toelating op basis van de Wtza SBV-Z mogen raadplegen om het BSN van cliënten te verifiëren.

Verder is onduidelijk of het wetsvoorstel vereisten zal bevatten over de opbouw van de identificatie en/of het standaardiseren daarvan. Een voorbeeld is (de mogelijkheid van) een koppeling tussen de identificatie en de rol van de zorgmedewerker, inclusief een standaardisatie van de mogelijke rollen. Voor het toepassen van autorisatie bij uitwisseling moeten zorgaanbieders afspraken maken over de rollen. Standaardisatie van rollen vergemakkelijkt het maken van die afspraken.

Artikelgewijze input

- **Artikel 14a lid 2.** Dit artikel zou moeten verduidelijken dat gebruik van een goedgekeurd inlogmiddel op zichzelf niet voldoende is voor het verkrijgen van toegang tot een elektronisch uitwisselingssysteem en zorginformatiesysteem. Voor veilige en vertrouwde toegang is meer nodig dan enkel gebruik van een goedgekeurd inlogmiddel, zoals dat sprake is van de juiste autorisatie. Wenselijk is dat de tekst van het artikel duidelijker wordt beperkt tot het inloggen als zodanig.

- **Artikel 14a lid 4.** Dit artikel lijkt ruimte te bieden om in onderliggende regelgeving eisen te stellen aan het verkrijgen van toegang tot een elektronisch uitwisselingssysteem en zorginformatiesysteem. Mogelijk is hiermee bedoeld om de toepassing van de overige generieke normen die nu worden opgesteld voor toestemming en lokalisatie op termijn verplicht te stellen. Of dat de bedoeling is, blijkt niet uit dit wetsvoorstel. Verduidelijking is gewenst.