HOOGHIEMSTRA & PARTNERS
strategisch en juridisch advies

Oplossingsrichtingen voor betrouwbaar en gebruiksvriendelijk inloggen bij hybride zorg

Theo Hooghiemstra, Helen Hukshorn en Riëlle Osepa

Inhoudsopgave

Lijst van afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
Bdo	Wetsvoorstel Besluit digitale overheid
BSN	Burgerservicenummer
BW	Burgerlijk Wetboek van Nederland
BZK	Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CBP	College bescherming persoonsgegevens
Conceptbesluit identificatiemiddelen	Conceptbesluit identificatiemiddelen voor burgers Wdo
Conceptregeling identificatiemiddelen	Conceptregeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo
ECD	Elektronisch cliënten dossier
EER	Europese Economische Ruimte
EHRM	Europese Hof voor de Rechten van de Mens
eID	Elektronische identificatiemiddelen of Elektronische identiteit
eIDAS 2.0	Voorstel voor een Verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit of de herziene eIDAS-verordening
eIDAS-verordening	Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische

	transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG
EPD	Elektronisch patiënten dossier
EU	Europese Unie
GGZ	Geestelijke gezondheidszorg
IZA	Integraal Zorgakkoord
Regeling betrouwbaarheidsniveaus	Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening of Regeling van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 8 mei 2023, nr. 23-0000244782, houdende regels betreffende de bepaling van het vereiste betrouwbaarheidsniveau van authenticatie voor de verlening van elektronisch diensten en overgangsrecht met betrekking tot betrouwbaarheidsniveaus
SSO	Single sign-on
TVS	ToegangVerleningService
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
VWS	De minister en/of het ministerie van Volksgezondheid, Welzijn en Sport
Wabvpz	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
Wallet	European Digital Identity Wallet
Wbp	Wet bescherming persoonsgegevens. Deze wet is per 25 mei 2018 vervallen.
Wdo	Wet digitale overheid of Wet tot algemene regels inzake het elektronisch verkeer in het

	publieke domein en inzake de generieke digitale infrastructuur
WGBO	Wet geneeskundige behandelingsovereenkomst

Managementsamenvatting

In de zorg bestaat de angst dat de op 1 juli jongstleden in werking getreden Wet digitale overheid (Wdo) het gebruiksgemak voor patiënten bij inloggen zal tegenwerken. Gevreesd wordt dat als gevolg hiervan de doelstellingen uit het Integraal Zorgakkoord voor hybride zorg niet gehaald worden. In het bijzonder zijn er zorgen over de inlogmiddelen en de verplichte betrouwbaarheidsniveaus.

Knelpunten en zorgen

Er is een groot aantal interviews gehouden met verschillende stakeholders. In deze interviews is ingegaan op waar de zorgen zitten bij de betreffende partijen en welke knelpunten zij zien als het gaat om het gebruik van de vereiste betrouwbaarheidsniveaus voor digitale dienstverlening en de verplichte acceptatie van erkende middelen vanuit de Wdo.

Uit de interviews blijkt dat er sprake is van verschillende knelpunten en zorgen, afhankelijk van welke stakeholder je spreekt. De knelpunten en zorgen bevinden zich op de volgende terreinen:

- het invoeren van een hoger betrouwbaarheidsniveau leidt tot afname van het gebruiksgemak en daarmee afname van het gebruik;
- er moeten verschillende middelen worden gebruikt voor verschillende toepassingen (dit is een knelpunt voor zowel de patiënt als de zorgverlener);
- de acceptatieplicht van DigiD, waarbij de voorwaarden voor het aansluiten een knelpunt vormen als het gaat om netwerkzorg; en
- het financieringsmodel bij inlogmiddelen, waarbij er onduidelijkheid bestaat over de procedure en de planning m.b.t. de erkenning.

Nieuw in de Wdo: acceptatieplicht en Stelsel Toegang

De vereisten in de Wdo als het gaat om betrouwbaarheidsniveaus zijn niet nieuw. Deze vloeiden al voort uit bestaande juridische kaders. Zoals de eisen die worden gesteld vanuit de (U)AVG als het gaat om het verwerken van gezondheidsgegevens en vereisten op grond van het medisch beroepsgeheim.

Wél nieuw in de Wdo is de nog niet in werking zijnde acceptatieplicht die de Wdo kent als het gaat om erkende en toegelaten middelen in het publieke domein. Ook nieuw is het gebruik van het Stelsel Toegang dat onder verantwoordelijkheid van BZK wordt gerealiseerd. In de zorg bestaat de angst dat de Wdo - in het bijzonder de inlogmiddelen - en de verplichte betrouwbaarheidsniveaus vanuit de eIDAS-verordening [1] het gebruiksgemak dusdanig zal tegenwerken dat deze digitale zorg niet gebruikt zal worden door patiënten en daarmee de doelstellingen uit het IZA voor hybride zorg niet gehaald kunnen worden.

[1] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. eIDAS staat voor Electronic Identities and Trust Services.

Oplossingsrichtingen

Het betrouwbaarheidsniveau eIDAS Hoog is momenteel nog niet breed beschikbaar voor patiënten/burgers. BZK zal het in de komende jaren nader ontwikkelen op basis van het Stelsel Toegang van BZK. Dit stelsel is dus nog niet gereed. Er zijn wel gebruiksvriendelijke private middelen gebaseerd op de meest moderne (mobiele) technologieën op betrouwbaarheidsniveau hoog beschikbaar, maar deze zijn nog niet erkend onder de Wdo. Bovendien is daar nog geen financiering voor, waardoor deze middelen (nog) niet breed beschikbaar zijn. Ook voor nutsmiddelen is nog geen Wdo-erkenning en publieke financiering beschikbaar.

Het lijkt daarmee onwaarschijnlijk dat de acceptatieplicht van erkende en toegelaten middelen vanuit de Wdo op korte termijn in werking zal treden.

Tegelijkertijd hebben de geïnterviewden aangegeven dat zij belang hechten aan een balans tussen vertrouwen en gebruiksvriendelijkheid. Om die reden lijkt het niet raadzaam om veel zorgaanbieders op betrouwbaarheidsniveau laag te houden totdat BZK het Stelsel Toegang gereed heeft en middelen op eIDAS Hoog breed beschikbaar zijn. Op basis van de gehouden interviews, literatuurstudie en onze eigen kennis en ervaring komen we tot onderstaande oplossingsrichtingen. Bij de indeling hiervan hebben we nadrukkelijk rekening gehouden met de tijdslijnen van het Integraal Zorgakkoord met betrekking tot hybride zorg.

De oplossingsrichtingen zijn verdeeld in twee categorieën, vullen elkaar aan en kunnen naast elkaar worden geïmplementeerd:

- oplossingsrichtingen op korte termijn; en
- oplossingsrichtingen op langere termijn.

De oplossingsrichtingen op korte termijn zijn:

- gefaseerd invoeren van het betrouwbaarheidsniveau substantieel;
- opschalen van bestaande ondersteuningsvormen;
- gebruikmaken van technologische oplossingen die al kunnen en zijn toegestaan;
- aanpassen wet- en regelgeving; en
- communiceren van alle authenticatiemogelijkheden.

De oplossingsrichtingen op langere termijn zijn:

- gefaseerd invoeren van het betrouwbaarheidsniveau hoog;
- gebruikmaken van technologische oplossingen (mobile first, biometrie en Wallet); en aanpassen van wet- en regelgeving.

1. Achtergrond, opdrachtomschrijving en aanpak

1.1 Achtergrond

Zoals opgenomen in het Integraal Zorgakkoord ("**IZA**") is een transformatie nodig naar hybride zorg om de zorg toegankelijk, kwalitatief en betaalbaar te houden.[2] De Wet digitale overheid ("**Wdo**") is op 1 juli 2023 gefaseerd in werking getreden. Dit leidt tot nieuwe vragen vanuit het zorgveld over de toepassing van de Wdo en de betrouwbaarheidsniveaus als het gaat om de inzet van digitale/hybride zorg. In de zorg bestaat de angst dat de Wdo - in het bijzonder de inlogmiddelen - en de verplichte betrouwbaarheidsniveaus vanuit de eIDAS-verordening [3] het gebruiksgemak dusdanig zal tegenwerken dat deze digitale zorg niet gebruikt zal worden door patiënten en daarmee de doelstellingen uit het IZA voor hybride zorg niet gehaald kunnen worden.

Zoals in het IZA is beschreven, betekent passende zorg steeds vaker ook hybride zorg: een mix van digitaal en fysiek aangeboden zorg en ondersteuning van gezondheid, waar mogelijk gepersonaliseerd en op maat. Uitgangspunten hierbij zijn: "*zelf als het kan, thuis als het kan en digitaal als het kan. Partijen werken samen aan brede opschaling en toepassing van hybride zorg*".[4]

Het doel is dat de inzet van hybride zorg in 2026 leidt tot aantoonbaar anders werken en het verlagen van de werkdruk van de zorgverleners met toegankelijkheids- en kwaliteitsbehoud. In onderdeel I van het IZA staat dat sectoren zullen onderzoeken welke zorgpaden geschikt zijn voor digitale en/of hybride zorg. Van deze geschikte zorg komt 70% digitaal of hybride beschikbaar. Van alle zorg die hybride wordt aangeboden, wordt op basis van het IZA gestreefd naar een inclusie van c.q. het gebruik door minimaal 50% van de patiëntenpopulatie waarvoor de hybride zorgpaden geschikt zijn. Hiertoe worden sectorale afspraken gemaakt. In het IZA wordt benadrukt dat veldpartijen zorgen dat de hybride zorg toegankelijk is voor mensen en dat inclusiviteit van deze zorg wordt bevorderd. Overheidspartijen faciliteren deze ontwikkeling.[5]

De inwerkingtreding van de Wdo leidt in het zorgveld tot nieuwe vragen, echter de vereisten die worden gesteld als het gaat om betrouwbaarheidsniveaus voor digitale dienstverlening door zorgaanbieders zijn niet nieuw. Deze vloeiden al voort uit bestaande juridische kaders zoals de eisen die worden gesteld vanuit de (U)AVG als het gaat om het verwerken van bijzondere persoonsgegevens, zoals gezondheidsgegevens en persoonsgegevens die vallen onder het medisch beroepsgeheim. Wat wél nieuw is, is de acceptatieplicht die de Wdo kent (nog niet in werking) als het gaat om erkende middelen in het publieke domein en het gebruik van het stelsel voor Toegang

[2] Integraal Zorg Akkoord, 'Samen werken aan gezonde zorg', september 2022, p. 92 en 95.

[3] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. eIDAS staat voor Electronic Identities and Trust Services.

[4] Integraal Zorg Akkoord, 'Samen werken aan gezonde zorg', september 2022, p. 15.

[5] Integraal Zorg Akkoord, 'Samen werken aan gezonde zorg', september 2022, p. 92 en 96.

dat onder verantwoordelijkheid van BZK wordt gerealiseerd. In deze notitie zal nader worden ingegaan op het juridisch kader en wat dit nu daadwerkelijk betekent in de praktijk.

Los van de wettelijke vereisten is het belangrijk dat hybride zorg op een veilige en betrouwbare manier voor de patiënten en zorgaanbieders geleverd kan worden. Het gaat tenslotte over medische gegevens van de patiënt die onder het medisch beroepsgeheim vallen. Het gaat om de integriteit van de behandelrelatie tussen patiënt en zorgverlener. Vertrouwen van patiënten dat zorgvuldig wordt omgegaan met hun gegevens is van groot belang voor de bereidheid om gebruik te maken van hybride zorg. Daar valt de identificatie en authenticatie van patiënten ook onder.

Tegelijkertijd is het belangrijk dat de hybride zorg toegankelijk is voor patiënten en dat deze toegankelijkheid voor juist de kwetsbare groepen in onze samenleving niet wordt gefrustreerd doordat de middelen niet gebruiksvriendelijk zijn. Als het té lastig is voor een patiënt om een digitale toepassing te gebruiken, bijvoorbeeld doordat het inloggen op een vereist betrouwbaarheidsniveau zeer gebruiksonvriendelijk is of een middel (nog) niet breed beschikbaar is, neemt de kans dat de patiënt geen gebruik maakt (of kan maken) van hybride zorg toe. Dit kan het halen van de IZA-doelstellingen frustreren.

Momenteel is het (helaas) nog niet zo dat een gebruiksvriendelijk middel op betrouwbaarheidsniveau hoog breed beschikbaar is voor de Nederlandse bevolking.[6] Als dat wél zo was, zou bovenstaand vraagstuk niet spelen. Uiteindelijk moeten we daar wel naartoe. De komende (overgangs)periode is het daarmee de uitdaging voor alle betrokken stakeholders (VWS, BZK, zorgaanbieders en leveranciers) om een balans te vinden tussen betrouwbaarheid en veiligheid van inlogmiddelen en het gebruiksgemak daarvan.

1.2 Opdrachtomschrijving

In het kader van het bovengenoemde heeft VWS Hooghiemstra & Partners benaderd met het verzoek om aan de hand van door het zorgveld aangeleverde casuïstiek uit de praktijk oplossingsrichtingen aan te leveren over welke betrouwbaarheidsniveaus onder de bestaande wetgeving (inclusief de Wdo) vereist zijn en op welke wijze deze kunnen worden ingevuld, zodat de identificatie en authenticatie van de patiënt het gebruiksgemak niet in de weg staat. Met andere woorden; welke oplossingsmogelijkheden zijn er om het gebruiksgemak te behouden en tegelijkertijd te borgen dat de hybride zorg op een veilige en betrouwbare manier wordt geleverd aan de patiënt?

[6] Zie ook Regeling van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 8 mei 2023, nr. 23-0000244782, houdende regels betreffende de bepaling van het vereiste betrouwbaarheidsniveau van authenticatie voor de verlening van elektronisch diensten en overgangsrecht met betrekking tot betrouwbaarheidsniveaus (Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening) (Stcrt 2023, 13656): *"Echter, de ontwikkeling van de digitale overheid en het breed beschikbaar maken van inlogmiddelen op hogere betrouwbaarheidsniveaus is een proces dat continu doorloopt, en zich stapsgewijs voltrekt. Het ligt in de verwachting dat op het moment van inwerkingtreding van de wet nog een aanloopperiode nodig is, omdat nog niet op alle betrouwbaarheidsniveaus de benodigde inlogmiddelen direct breed beschikbaar zullen zijn".*

Deze oplossingen kunnen zowel in wetgeving, als in techniek, ontwerp of aanvullende mitigerende maatregelen gezocht worden.

1.3 Aanpak

Ter uitvoering van de opdracht heeft Hooghiemstra & Partners onderstaande aanpak gehanteerd.

1. Houden van interviews met een brede groep vertegenwoordigers van stakeholders, zoals (zie voor een totaaloverzicht bijlage 3):
    a) zorgorganisaties;
    b) burgers/patiënten;
    c) technologische innovatieve bedrijven op het terrein van Identity Management;
    d) zorgtechnologie bedrijven die hybride zorgtoepassingen leveren;
    e) medeoverheden, zoals BZK en Logius;
    f) experts op het gebied van identificatie en authenticatie; en
    g) stakeholders en experts binnen VWS (beleidsverantwoordelijken van andere directies en juristen).
2. Literatuurstudie op basis van alle relevante documentatie. Een update van het geldende juridische kader is opgesteld met betrekking tot de betrouwbaarheidsniveaus in de zorg. Een analyse is gemaakt van de vereiste betrouwbaarheidsniveaus onder de bestaande wetgeving aan de hand van door het zorgveld aangeleverde casuïstiek uit de praktijk.
3. Analyseren en uitwerken van de concept bevindingen en oplossingsrichtingen.
4. De concept oplossingsrichtingen zijn getoetst bij de opdrachtgever, de IZA-tafel en in een aantal consultatiesessies met (een deel van) de geïnterviewden.
5. De concept oplossingsrichtingen zijn nader uitgewerkt, de feedback is verwerkt en de concept oplossingsrichtingen zijn voorgelegd aan de opdrachtgever.
6. Het definitieve rapport met het juridisch kader, analyse vereiste betrouwbaarheidsniveaus casuïstiek en de definitieve oplossingsrichtingen is opgeleverd.

2. Zorgen en knelpunten zorgveld, patiënten en leveranciers

Zoals aangegeven in de aanpak van deze opdracht, is een groot aantal interviews gehouden met verschillende stakeholders. De interviews zijn gehouden met vertegenwoordigers vanuit het zorgveld, patiënten, zorgtechnologiebedrijven die toepassingen leveren die gebruikt worden in de zorg, technologisch innovatieve bedrijven op het terrein van Identity Management, medeoverheden met relevante verantwoordelijkheden, zoals BZK en Logius en experts op het gebied van zorg en digitale toegang. In deze interviews is ingegaan op waar de zorgen zitten bij de betreffende partijen en welke knelpunten zij zien als het gaat om het gebruik van de vereiste betrouwbaarheidsniveaus voor digitale dienstverlening en de verplichte acceptatie van erkende middelen vanuit de Wdo.

Uit de interviews blijkt dat er sprake is van verschillende knelpunten en zorgen, afhankelijk van welke stakeholder je spreekt. Het is van belang om dit onderscheid goed helder te hebben voordat wordt gekeken naar de oplossingen.

2.1 Door hoger betrouwbaarheidsniveau, afname gebruiksgemak en daarmee gebruik

In het zorgveld bestaat de angst dat de Wdo - in het bijzonder de inlogmiddelen - en de verplichte betrouwbaarheidsniveaus vanuit de eIDAS-verordening het gebruiksgemak dusdanig zal tegenwerken dat deze digitale zorg niet gebruikt zal worden (of kan worden) door patiënten en daarmee de doelstellingen uit het IZA voor hybride zorg niet gehaald kunnen worden. Dit omdat wordt voorzien dat voor het overgrote deel van de digitale dienstverlening betrouwbaarheidsniveau eIDAS Hoog vereist is en men het huidige DigiD Hoog als gebruiksonvriendelijk ziet. Deze zorg is er ook als het gaat om afname van het bestaande gebruik van zorgportalen en hybride zorg-toepassingen die al worden ingezet, zoals thuismetingen, thuisbehandeling, digitale communicatie en beeldbellen. Voor bijna alle diensten van zorgaanbieders voor patiënten geldt dat momenteel ingelogd kan worden door de patiënt met een middel op betrouwbaarheidsniveau eIDAS Laag (DigiD Laag of een ander inlogmiddel op betrouwbaarheidsniveau laag). Daarnaast werkt een aantal zorgaanbieders met een door henzelf ontwikkeld middel, dat goed aanslaat bij de patiënten en geïntegreerd is in de zorgprocessen. Daar is de zorg wat het effect gaat worden van de inwerkingtreding van de Wdo; mag het eigen middel nog wel worden gebruikt?

Voor patiënten geldt een vergelijkbare zorg. Deze is niet beperkt tot het inloggen, maar strekt zich ook uit tot de inzet van hybride zorg in den brede. Het voordeel van hybride zorg wordt breed erkend en levert voor patiënten veel op. Echter, grote delen van de bevolking hebben nu al veel moeite met het gebruik van digitale toepassingen.[7] Veel ondersteuning is nodig voor deze groepen in de overgangsfase naar hybride zorg (bijvoorbeeld via bibliotheken, balie bij zorgaanbieders, welzijnsorganisaties en helpdeskdigitalezorg.nl). Voor een deel van de mensen zal deze

[7] Zie ook NOS Nieuws (B. de Vries), 'Miljoenen snappen digitale overheid onvoldoende, meeste hoofdpijn over DigiD', 10 juli 2023.

ondersteuning structureel nodig blijven. Dit om te voorkomen dat de zorg voor deze groepen niet in gelijke mate toegankelijk is (inclusie).

2.2 Verschillende middelen: knelpunt patiënt en zorgverlener

Vanuit de organisaties die de gebruiker goed kennen (burger, patiënt) wordt het ook als een voordeel gezien als er een of meerdere middelen op betrouwbaarheidsniveau hoog (of substantieel) komen die overal gebruikt kunnen worden; dat maakt het eenvoudiger. Uiteraard is gebruiksvriendelijkheid dan wel een voorwaarde. Nu zijn er veel verschillende manieren waarop men moet inloggen bij toepassingen die worden gebruikt/voorgeschreven door verschillende zorgaanbieders. In bijvoorbeeld de thuiszorg wordt dit tevens gezien als een knelpunt voor de hulpverleners die door patiënten gevraagd worden om te ondersteunen bij het gebruik van de verschillende toepassingen die thuis worden ingezet. Hetzelfde knelpunt komt in de interviews naar voren als het gaat om de persoonlijke gezondheidsomgevingen (PGO's) aangezien de patiënt bij het PGO niet kan inloggen met DigiD maar vervolgens bij het ophalen van de gegevens bij de zorgaanbieder vaak wel DigiD moet gebruiken of weer een ander inlogmiddel.

2.3 Verplichte acceptatie DigiD, voorwaarden aansluiten knelpunt

Een knelpunt dat veel naar voren komt, ziet niet zozeer op het verhogen van het betrouwbaarheidsniveau maar op de voorwaarden die worden gesteld als een acceptatieplicht gaat gelden voor DigiD. De zorgtechnologiebedrijven (leverancier van de zorgaanbieder) zoals bijvoorbeeld BeterDichtbij en Luscii bieden toepassingen die door de zorgaanbieders worden ingezet voor het leveren van hybride zorg. Vaak gebruiken deze leveranciers nu een 'eigen' middel (tweefactor, eIDAS laag).

Een belangrijk knelpunt dat deze leveranciers voorzien, heeft niet zozeer te maken met het betrouwbaarheidsniveau, maar met de acceptatieplicht van zorgaanbieders die gaat gelden voor erkende en toegelaten middelen, zoals opgenomen in de eerste tranche van de Wdo.[8] Met name het verplichte gebruik van DigiD en de voorwaarden die daaraan worden gesteld, verhoudt zich niet goed tot het concept dat door een aantal aanbieders is gekozen voor de toepassing. Het concept is vaak gebaseerd op het gebruiksgemak van de patiënt die zich beweegt in een netwerk van zorg. Zorg wordt steeds vaker regionaal geleverd en niet meer door één organisatie. Dit betekent dat de patiënt inlogt en vervolgens de toepassing kan gebruiken voor alle zorgaanbieders waar een behandelrelatie mee is en die werken met de betreffende toepassing. De voorwaarden die door Logius worden gesteld aan het gebruik van DigiD staan dit niet toe.[9] Bij een aansluiting op DigiD moet de patiënt bijvoorbeeld per zorgaanbieder (domein) apart inloggen. Voor zorgportalen is dit geen knelpunt; daar wordt alleen op het specifieke domein ingelogd.

[8] Zie artikel 7 Wdo. Dit artikel is nog niet in werking getreden.

[9] Deze voorwaarden volgen met name eisen die voortkomen uit wet- en regelgeving maar zijn ook deels een interpretatie daarvan waarbij nog wel (beperkt) ruimte bestaat om af te wijken.

Binnen de Geestelijke gezondheidszorg ("**GGZ**") wordt daarnaast nog gewezen op het volgende knelpunt bij het gebruik van DigiD. DigiD biedt de mogelijkheid tot 'eenmalig inloggen' (eenvoudige herauthenticatie). Burgers hoeven dan tijdens een actieve sessie niet opnieuw in te loggen als ze wisselen tussen webdiensten in hetzelfde domein.[10] De cliënt logt dan bijvoorbeeld in bij de GGZ-instelling en kan dan gebruik maken van de verschillende toepassingen binnen de omgeving, bijvoorbeeld beeldbellen en e-coaching. Echter, dit is nu zo ingericht dat de cliënt bij 15 minuten inactiviteit moet herauthenticeren anders wordt de eenmalig inloggen sessie bij DigiD ongeldig (en wordt de cliënt automatisch uitgelogd). [11]Dat is met name tijdens een behandeling onwenselijk en daardoor is DigiD volgens enkele geïnterviewden niet goed bruikbaar.

Wél wordt de naamsbekendheid van DigiD als een groot voordeel gezien. De zorg is dan wel weer dat dit weinig ruimte biedt aan andere private middelen, omdat die niet zo bekend zijn en vertrouwd worden als DigiD.

2.4 Financieringsmodel inlogmiddelen, onduidelijkheid procedure en planning erkenning

Technologisch innovatieve bedrijven op het terrein van Identity Management hebben met name veel vragen over de wijze van financiering van andere inlogmiddelen voor het publieke domein dan DigiD. De Wdo geeft nadrukkelijk de mogelijkheid voor private middelen om ingezet te kunnen worden in het publieke domein.[12] Deze moeten dan worden erkend door BZK.[13] DigiD is nu gratis voor burgers. Ook voor de private middelen gaat gelden dat ze binnen het Wdo domein gratis moeten zijn. DigiD mag niet buiten het Wdo-domein worden ingezet. Private middelen mogen dat wel en mogen daar ook kosten voor rekenen.

Voor het gebruik van DigiD door de zorgaanbieders zijn in de huidige situatie afspraken gemaakt over de financiering van de kosten voor de zorgaanbieder. Deze worden gedragen door het ministerie van VWS. Indien een dergelijke compensatie niet voor private middelen geldt, is er geen business case voor hen. Het is de vraag of er dan private inlogmiddelen op substantieel en hoog worden ontwikkeld. Zorgaanbieders zullen niet kiezen voor een middel dat geld kost als er een 'gratis' alternatief is. Uiteraard is dit anders nadat de acceptatieplicht van kracht wordt, dan moeten zorgaanbieders alle erkende middelen accepteren.
Daarnaast bestaat er nog onduidelijkheid bij bedrijven over de planning en het proces van het erkennen van private middelen die gebruikt zouden kunnen worden binnen het Stelsel Toegang en de eisen die gesteld zullen worden door BZK.

[10] Logius, 'Handleiding voor aansluiten op DigiD', onder Keuze Eenmalig inloggen.

[11] Logius, 'Koppelvlakspecificatie DigiD SAML Authenticatie', onder Herauthenticate en timers.

[12] Zie artikel 9 Wdo. Dit artikel is nog niet in werking getreden.

[13] Zie artikel 11 Wdo. Dit artikel is nog niet in werking getreden.

3. Juridisch kader en uitwerking van de casuïstiek

3.1 Juridisch kader: samenvatting

Onderstaand is het juridisch kader met betrekking tot het bepalen van de vereiste betrouwbaarheidsniveaus voor elektronische dienstverlening in de zorg op hoofdlijnen beschreven. Hierbij ligt de focus op het bestaande kader als het gaat om het bepalen van betrouwbaarheidsniveaus en de effecten van de inwerkingtreding van de Wdo. Het nader uitgewerkte juridische kader is opgenomen in Bijlage 1 van dit rapport.

3.1.1 Passend beveiligingsniveau: (U)AVG

De AVG vereist dat persoonsgegevens op een rechtmatige, behoorlijke en transparante wijze worden verwerkt.[14] Persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.[15] Zie tevens artikel 32 AVG dat de verwerkingsverantwoordelijke en verwerker verplicht de persoonsgegevens die worden verwerkt te beveiligen door passende technische en organisatorische maatregelen te treffen.

Bij het bepalen van het vereiste betrouwbaarheidsniveau voor digitale dienstverlening door zorgaanbieders gaat het dus om de vraag *welk betrouwbaarheidsniveau kwalificeert als 'passend'* in de zin van de AVG. De maatregelen moeten in verhouding staan tot de aard van de gegevens die worden verwerkt en de bijbehorende risico's voor de betrokkenen. Hoe groter het risico voor betrokkenen, des te zwaarder de beveiligingsmaatregelen zijn die getroffen moeten worden. Er is bijvoorbeeld sprake van een hoog risico als op grote schaal bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens, worden verwerkt. Als het gaat om elektronische dienstverlening van zorgverleners aan patiënten kan hier al snel sprake van zijn. Het uitgangspunt is dat de zorgverlener (als verwerkingsverantwoordelijke) verantwoordelijk is – op basis van een risicoanalyse – voor het bepalen van het betrouwbaarheidsniveau van de verleende diensten.

Zoals nader uitgewerkt in Bijlage 1 heeft de Autoriteit Persoonsgegevens (**AP**, voorheen **CBP**) in een aantal voorbeeldcases criteria vastgesteld waarmee bepaald kan worden welk betrouwbaarheidsniveau voor digitale dienstverlening van zorgaanbieders van toepassing is. De conclusie is dat als het gaat om een nadere invulling van hetgeen als passend in de zin van artikel 5, eerste lid, sub f, AVG wordt aangemerkt, de AP voor de verwerking van persoonsgegevens waarop het medisch beroepsgeheim rust, uitgaat van het betrouwbaarheidsniveau hoog. [16]

---

[14] Artikel 5, eerste lid, sub a, AVG.

[15] Artikel 5, eerste lid, sub f, AVG.

[16] Autoriteit Persoonsgegevens, brief aan het Ministerie van Volksgezondheid, Welzijn en Sport, z2018-17577, 4 oktober 2018.

Ook in de Handreiking voor overheidsorganisaties: Betrouwbaarheidsniveaus voor digitale dienstverlening van het Forum Standaardisatie[17] (de "**Handreiking**") is opgenomen dat als het gaat om gegevens die onder het beroepsgeheim vallen (zoals medische gegevens) dient te worden uitgegaan van het betrouwbaarheidsniveau hoog. Als er sprake is van bijzondere persoonsgegevens (waaronder gezondheidsgegevens) die niet onder het beroepsgeheim vallen, dient volgens de Handreiking uit te worden gegaan van het betrouwbaarheidsniveau substantieel.

Voor de vraag welk betrouwbaarheidsniveau bij informatie-uitwisseling tussen zorgaanbieders en patiënten dient te worden toegepast is van belang óf sprake is van persoonsgegevens waarop het medisch beroepsgeheim van de zorgverlener rust (betrouwbaarheidsniveau hoog). In Bijlage 1 is dit nader toegelicht.

Gedoogsituatie zolang passend betrouwbaarheidsniveau patiëntauthenticatie niet mogelijk is

Sinds 2018 is er sprake van een gedoogsituatie. Het uitgangspunt van de AP is als volgt. *"Zolang een passend betrouwbaarheidsniveau voor patiëntauthenticatie niet kan worden gerealiseerd, mag elektronische uitwisseling van gegevens over gezondheid tussen zorgaanbieders en patiënten in beginsel niet plaatsvinden. De bescherming van persoonsgegevens, waaronder gegevens over gezondheid, is dan onvoldoende gewaarborgd. Zodra binnen het eID-programma inlogmethoden met de betrouwbaarheidsniveaus "substantieel" en "hoog" breed beschikbaar komen, dient een lager betrouwbaarheidsniveau bij de verwerking van gegevens over gezondheid dus niet meer beschikbaar te worden gesteld."*[18]

De AP ziet echter in dat het niet in het belang van de patiënt is dat zorginnovaties stilstaan totdat de passende betrouwbaarheidsniveaus breed beschikbaar zijn binnen het eID-programma. *"Daarom is het in eerste instantie van belang dat de nodige voortvarendheid wordt betracht bij de ontwikkeling en het beschikbaar maken van de benodigde betrouwbaarheidsniveaus binnen het eID-stelsel. (…) Verder moet de zorgsector bezien welke mogelijkheden – eventueel buiten DigiD om – momenteel wél beschikbaar zijn om te gebruiken voor patiëntauthenticatie. (…) Zo wordt duidelijk op welke wijze het nieuwe eID-stelsel bij patiënten en zorgaanbieders kan worden geïmplementeerd.*

In afwachting van het breder beschikbaar komen van authenticatiemethoden met een passend hoog niveau, dient authenticatie plaats te vinden met tenminste tweefactorauthenticatie (zoals DigiD in combinatie met sms). Een lagere betrouwbaarheid is in ieder geval niet aanvaardbaar. Randvoorwaarde daarbij is dat er zo nodig aanvullende maatregelen worden getroffen om openstaande risico's, die niet worden weggenomen met tweefactorauthenticatie, te mitigeren."

Onduidelijk is wat wordt verstaan onder breed beschikbaar en wanneer hiervan sprake is.

---

[17] Forum Standaardisatie, 'Handreiking voor overheidsorganisaties: Betrouwbaarheidsniveaus voor digitale dienstverlening', november 2016.

[18] Autoriteit Persoonsgegevens, brief aan het Ministerie van Volksgezondheid, Welzijn en Sport, z2018-17577, 4 oktober 2018, par. 4 onder Uitgangspunt van de AP.

3.1.2 Inwerkingtreding Wdo

De Wet digitale overheid ("**Wdo**") is op 1 juli 2023 (gedeeltelijk) in werking getreden. Dit leidt tot nieuwe vragen vanuit het zorgveld over de toepassing van de Wdo en de betrouwbaarheidsniveaus als het gaat om de inzet van digitale/hybride zorg. In de zorg bestaat de angst dat de Wdo - in het bijzonder de inlogmiddelen - en de verplichte betrouwbaarheidsniveaus vanuit de eIDAS-verordening het gebruiksgemak dusdanig zal tegenwerken dat deze digitale zorg niet gebruikt zal worden door patiënten en daarmee de doelstellingen uit het IZA voor hybride zorg niet gehaald kunnen worden.

Wdo: gefaseerd in werking, eerste tranche

De Wdo ziet op de digitale overheid. Er is ervoor gekozen om de Wdo ook van toepassing te laten zijn op zorgaanbieders. Zorgaanbieders zijn aangewezen organisaties, zoals bedoeld in artikel 2, tweede lid, sub a, Wdo. In de bijlage bij artikel 2, tweede lid, onder a, Wdo is opgenomen dat de Wdo ook van toepassing is op zorgaanbieders, categorieën van indicatieorganen en categorieën van zorgverzekeraars die vallen onder de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg ("**Wabvpz**"), in het kader van de taken waarvoor zij op basis van de Wdo het burgerservicenummer ("**BSN**") gebruiken.

De Wdo is een kaderwet, uitwerking vindt plaats in de lagere regelgeving. Zoals in algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen. Hiervoor is gekozen om ruimte te laten voor innovatie, verdere keuzes en nieuwe voorzieningen en functionaliteiten.

Eerste tranche Wdo; nog niet veel nieuws voor zorgaanbieders

Als het gaat om de eerste tranche van de Wdo die op 1 juli 2023 in werking is getreden is met name artikel 6 Wdo van belang. Dit artikel ziet op de betrouwbaarheidsniveaus als het gaat om toegang tot elektronische dienstverlening. De Wdo volgt de betrouwbaarheidsniveaus van de eIDAS-verordening: laag, substantieel en hoog. In het eerste lid is geregeld dat bij elektronische dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, bestuursorganen en aangewezen organisaties uitsluitend toegang tot de dienstverlening verlenen indien gebruik wordt gemaakt van identificatiemiddelen die ten minste het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau hebben. Voor de zorgaanbieder betekent dit, als het gaat om het vereiste betrouwbaarheidsniveau niet echt iets nieuws. Zoals eerder beschreven is, was de zorgaanbieder ook voor de (gedeeltelijke) inwerkingtreding van de Wdo op grond van de AVG al verantwoordelijk om te zorgen voor een passend beveiligingsniveau. De Wdo concretiseert deze verplichting.

In artikel 6, tweede lid, Wdo is opgenomen dat bestuursorganen en aangewezen organisaties, zoals zorgaanbieders, volgens bij ministeriële regeling te stellen regels bepalen voor welke door hen te verlenen elektronische diensten authenticatie op een bepaald betrouwbaarheidsniveau vereist is. Dit is nader uitgewerkt in de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening ("**Regeling betrouwbaarheidsniveaus**").

Regeling betrouwbaarheidsniveaus
In de Regeling betrouwbaarheidsniveaus worden nadere regels gesteld over de criteria die door publieke dienstverleners moeten worden gehanteerd.[19] Deze regeling is 1 juli 2023 in werking getreden.

Op grond van artikel 2, tweede lid, Regeling betrouwbaarheidsniveaus juncto bijlage 2 bij de Regeling betrouwbaarheidsniveaus wordt geconcludeerd dat (in het geval niet bij wettelijk voorschrift is bepaald dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is) betrouwbaarheidsniveau hoog vereist is als het gaat om gegevens die onder het medisch beroepsgeheim vallen.

Op grond van artikel 2, derde lid, Regeling betrouwbaarheidsniveaus juncto bijlage 2 bij de Regeling betrouwbaarheidsniveaus wordt geconcludeerd dat (in het geval niet bij wettelijk voorschrift is bepaald dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is) betrouwbaarheidsniveau substantieel vereist is als het om bijzondere categorieën van persoonsgegevens (zoals gegevens over gezondheid)[20] gaat.

In bijlage 2 bij de Regeling betrouwbaarheidsniveaus is daarnaast opgenomen als criterium voor betrouwbaarheidsniveau hoog dat het BSN wordt verwerkt in combinatie met andere persoonsgegevens. De criteria die in de Wdo zijn opgenomen, komen overeen met de bovenstaand in paragraaf 3.1.1 reeds beschreven criteria.

Artikelen Wdo nog niet in werking: acceptatieplicht erkende middelen
Artikel 7 Wdo regelt de acceptatieplicht voor toegelaten en erkende identificatiemiddelen en digitale machtigingsverklaringen. [21] Voor de inwerkingtreding van dit artikel is van belang dat de ontwikkeling van de techniek (ICT) en de organisatie achter het Stelsel Toegang afgerond is. Uit gesprekken komt naar voren dat nog niet duidelijk is wanneer het Stelsel Toegang gereed is. Er wordt voorzien dat het meer tijd zal kosten dan in de oorspronkelijke planning opgenomen. De oorspronkelijke planning die nu nog wordt gecommuniceerd is als volgt: de techniek (ICT) en de organisatie achter het Stelsel Toegang zijn naar verwachting in 2024 klaar. Dat betekent dat het stelsel toegankelijk voor dienstverleners zou moeten zijn en dat inlogmiddelen erkend kunnen worden. Het is de bedoeling dat alle dienstverleners in de komende 3 jaar zich aansluiten op het stelsel. Ook is het de bedoeling dat alle overheidsorganisaties in de tweede helft van 2026 op het nieuwe stelsel over zijn.[22] Van belang is om zo snel als mogelijk duidelijkheid te krijgen over wanneer het Stelsel Toegang gereed is.

---

[19] Toelichting bij het Conceptbesluit identificatiemiddelen, par. 2.2.

[20] Artikel 1 Regeling betrouwbaarheidsniveaus juncto artikel 1 van de Uitvoeringswet Algemene verordening gegevensbescherming en artikel 9, eerste lid, AVG.

[21] Artikel 7 Wdo. Dit artikel is nog niet in werking getreden. Een toegelaten identificatiemiddel wordt in de Wdo omschreven als een identificatiemiddel voor een natuurlijke persoon dat is aangewezen ingevolge artikel 9 (Wdo).

[22] Digitale Overheid, 'Veelgestelde vragen over de inwerkingtreding van de Wdo'.

In artikel 7, tweede lid, Wdo (nog niet in werking) is het volgende opgenomen: aangewezen organisaties accepteren bij hun elektronische dienstverlening aan natuurlijke personen waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is uitsluitend:
a. alle toegelaten identificatiemiddelen;
b. elektronische verklaringen als bedoeld in artikel 5, eerste lid, onderdeel b; en
c. onverminderd het bepaalde in artikel 6 van de eIDAS-verordening, alle identificatiemiddelen die behoren tot een door een lidstaat van de Europese Unie ("**EU**") ingevolge de eIDAS-verordening bij de Europese Commissie aangemeld en goedgekeurd stelsel indien dit is bepaald bij besluit van Onze Minister in overeenstemming met Onze Minister die het mede aangaat.

Dit betekent voor zorgaanbieders dat nadat de acceptatieplicht van kracht is uitsluitend toegelaten en erkende identificatiemiddelen gebruikt mogen worden. Niet toegelaten en erkende middelen mogen daarmee dus niet meer worden geaccepteerd. Echter, in artikel 29, derde lid, Wdo wordt bepaald dat de in de artikel 7 Wdo opgenomen acceptatieplicht voor een aangewezen organisatie niet eerder van toepassing is dan nadat die aangewezen organisatie kan worden aangesloten op de in artikel 5, eerste lid, onderdelen a tot en met e, en tweede lid Wdo bedoelde infrastructuur en voorzieningen (die dan dus gereed moeten zijn) overeenkomstig het bij regeling van Onze Minister, gehoord Onze Ministers die het mede aangaat, op te stellen aansluitschema. Het aansluitschema kan erin voorzien dat de acceptatieplichten voor verschillende diensten van een bestuursorgaan of aangewezen organisatie op verschillende momenten van toepassing worden.

Voor de zorgaanbieder betekent dit dat ook nadat de acceptatieplicht in artikel 7 Wdo in werking treedt, deze niet eerder van toepassing is dan nadat de zorgaanbieder ook daadwerkelijk kan worden aangesloten op het Stelsel Toegang. Allereerst zal dit stelsel dan technisch en organisatorisch gereed moeten zijn (verantwoordelijkheid ministerie van BZK). Aansluiting zal dan plaatsvinden op basis van een aansluitschema. De Wdo gaat dus pas volledig gelden als een instantie technisch en organisatorisch klaar is om aan te sluiten. De departementen, de publieke dienstverleners en Logius stellen samen een aansluitschema op. Dit aansluitschema gaat een planning bevatten met data waarop de specifieke onderdelen van de wet voor welke instantie van kracht worden. [23]

3.2 Uitwerking van de casuïstiek: betrouwbaarheidsniveau patiëntauthenticatie

Bovenstaand is een samenvatting gegeven van het juridische kader dat geldt voor het bepalen van het vereiste betrouwbaarheidsniveau voor digitale dienstverlening door zorgaanbieders. In dit hoofdstuk wordt op basis van dit kader en de bijbehorende criteria voor de door het zorgveld voorgedragen casuïstiek nader ingegaan op de vraag welk betrouwbaarheidsniveau voor patiëntauthenticatie van toepassing is. Hiervoor geldt dat deze analyse plaatsvindt op basis van de aangeleverde casuïstiek die op hooflijnen is omschreven en per toepassing in de praktijk anders kan zijn. Het gaat dus om een analyse op hoofdlijnen en niet van specifieke systemen. Ook wordt in deze

[23] Digitale overheid, 'Wet digitale overheid'.

analyse niet meegenomen in hoeverre eventueel risicoverlagende of risicoverhogende omstandigheden van toepassing zijn, zoals bijvoorbeeld andere technische of organisatorische maatregelen. De onderzoeksvraag naar het betrouwbaarheidsniveau van de patiënttoegang is feitelijk een analyse van de beschikbare aanwijzingen van het risico van de gegevensverwerkingen in het algemeen. Bijzonderheden van het concrete geval kunnen het noodzakelijke betrouwbaarheidsniveau beïnvloeden. De verwerkingsverantwoordelijke is degene die zorg moet dragen voor passende beveiliging en bescherming van persoonsgegevens die hij verwerkt.

3.2.1 Thuismetingen

Thuismetingen worden gedaan voor zowel actuele telemonitoring, als voor controle achteraf (trends in de gaten houden). Bij telemonitoring worden gegevens gebruikt om (continu) in de gaten te houden of er medische actie vanuit een zorgverlener nodig is.

- Zelf registratie in een app van de leverancier van de meetapparatuur.
  De patiënt meet zelf (bijvoorbeeld gewicht, hartslag, bloeddruk en bloedsuikerspiegel) en registreert deze data in een app. De gegevens komen dan in het persoonlijke dossier van die patiënt (in de Cloud-omgeving van de leverancier van de meetapparatuur). Daarna zijn er twee opties:
  - De zorgverlener krijgt toegang tot deze gegevens door in te loggen in het systeem van de app-leverancier; of
  - Er is een koppeling met het EPD/ECD[24]-systeem van de zorgaanbieder en de gegevens worden automatisch doorgestuurd naar het EPD/ECD.
- Koppeling van apparaat/sensor en telefoon (via bluetooth/ internet)

  Het meetapparaat (bijvoorbeeld Hartritmesensor of bloedglucose sensor) maakt een verbinding met de telefoon van de patiënt en stuurt de meetgegevens (continue/periodiek) door naar het dossier van de patiënt in de Cloud van de leverancier van de meetapparatuur. Daarna zijn er twee opties:

  - De zorgverlener krijgt toegang tot deze gegevens door in te loggen in het systeem van de app-leverancier; of
  - Er is een koppeling met het EPD/ECD-systeem van de zorgaanbieder en de gegevens worden automatisch doorgestuurd naar het EPD/ECD.
  - Om de gegevens zelf in te zien, zal de patiënt een app moeten openen en eventueel een nieuwe meting moeten uitvoeren.

Casus: thuismetingen, zelfregistratie in app leverancier	
AVG-rol leverancier	**Betrouwbaarheidsniveau**
Verwerker van de zorgaanbieder	- de thuismetingen maken deel uit van de behandeling van de zorgverlener. - de leverancier werkt onder verantwoordelijkheid van de

	zorgaanbieder. - de gegevens die door de patiënt worden ingevoerd en verstuurd vallen onder het medisch beroepsgeheim. - Het muteren van het medisch dossier brengt over het algemeen meer risico's met zich mee dan alleen inzage. Onder andere vanwege de denkbare gevolgen voor het gebruik van de gemuteerde gegevens voor de zorgverlening. [25] - Er is sprake van het verwerken van het BSN in combinatie met gezondheidsgegevens. **Betrouwbaarheidsniveau hoog is vereist**
Verwerkingsverantwoordelijke	- Het zou zo kunnen zijn dat de patiënt zelf beheerde medische gegevens met de zorgaanbieder wenst te delen en daarvoor gebruik maakt van een zelf aangeschafte toepassing van een leverancier. In dat geval is de leverancier verwerkingsverantwoordelijke en vallen deze gegevens niet onder het medisch beroepsgeheim zolang ze niet gedeeld worden met de zorgaanbieder. - Er worden bijzondere persoonsgegevens verwerkt, potentieel grootschalig. - Er wordt geen BSN verwerkt, leverancier kan niet meeliften op de grondslag van de zorgaanbieder. **Minimaal betrouwbaarheidsniveau substantieel is vereist.**

[25] PrivacyCare en PBLQ, 'Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg', mei 2016, p. 40.

Casus: thuismetingen, koppeling apparaat/sensor en telefoon (via bluetooth/internet)	
AVG-rol leverancier	**Betrouwbaarheidsniveau**
Verwerker van de zorgaanbieder	- de thuismetingen maken deel uit van de behandeling van de zorgverlener. - de leverancier werkt onder verantwoordelijkheid van de zorgaanbieder. - de gegevens die door de toepassing worden ingevoerd en verstuurd vallen onder het medisch beroepsgeheim. - Het muteren van het medisch dossier brengt over het algemeen meer risico's met zich mee dan alleen inzage. Onder andere vanwege de denkbare gevolgen voor het gebruik van de gemuteerde gegevens voor de zorgverlening. [26] - Er is sprake van het verwerken van het BSN in combinatie met gezondheidsgegevens. - Het zou bij deze casus zo kunnen zijn dat er sprake is van 'machine to machine' uitwisseling. Dan is de vraag of de patiënt wordt gevraagd om in te loggen. Zo nee, dan is de vraag m.b.t. betrouwbaarheidsniveau niet van toepassing. - Indien deze werkwijze wél vereist dat moet worden ingelogd door de patiënt dan geldt hetzelfde als bij zelfregistratie bij app leverancier. **Betrouwbaarheidsniveau hoog is vereist**
Verwerkingsverantwoordelijke	Deze optie zal niet snel voorkomen aangezien de patiënt dan zou moeten beschikken over eigen meetapparatuur die ten behoeve van de behandelrelatie wordt ingezet op initiatief van de patiënt.

[26] PrivacyCare en PBLQ, 'Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg', mei 2016, p. 40.

3.2.2 Thuisbehandeling

De patiënt krijgt apparatuur van de zorgaanbieder (bijvoorbeeld een dialyseapparaat) en voert zelf een behandeling uit. Indien er gegevens worden verwerkt, gebeurt dit zoals hiervoor beschreven bij 'thuismeting'.

Casus: thuisbehandeling	
AVG-rol van de leverancier	**Betrouwbaarheidsniveau**
Verwerker van de zorgaanbieder	Indien gegevens worden verwerkt, geldt het hetzelfde als bij de casus thuismetingen. - de patiënt voert in het kader van de behandeling zélf een deel daarvan thuis uit. De apparatuur wordt door de zorgverlener ter beschikking gesteld. - de leverancier werkt onder verantwoordelijkheid van de zorgaanbieder. - de gegevens die door de toepassing worden ingevoerd en verstuurd vallen onder het medisch beroepsgeheim. - Het muteren van het medisch dossier brengt over het algemeen meer risico's met zich mee dan alleen inzage. Onder andere vanwege de denkbare gevolgen voor het gebruik van de gemuteerde gegevens voor de zorgverlening. [27] - Er is sprake van het verwerken van het BSN in combinatie met gezondheidsgegevens. - Het zou bij deze casus ook zo kunnen zijn dat er sprake is van 'machine to machine' uitwisseling. Dan is de vraag of de patiënt wordt gevraagd om in te loggen. Zo nee, dan is de vraag m.b.t. betrouwbaarheidsniveau niet van toepassing. - Indien deze werkwijze wél vereist dat moet worden ingelogd door de patiënt dan geldt hetzelfde als bij zelfregistratie bij app leverancier. **Betrouwbaarheidsniveau hoog is vereist**

[27] PrivacyCare en PBLQ, 'Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg', mei 2016, p. 40.

Verwerkingsverantwoordelijke	Deze optie zal niet snel voorkomen aangezien de patiënt op eigen initiatief zou moeten besluiten om gegevens via een toepassing te gaan versturen naar de zorgverlener.

3.2.3 eCoaches

Via een app krijgt de patiënt informatie van een eCoach die past bij het ziektebeeld en de fase waarin de patiënt zich bevindt. Deze eCoach kan een voorgeprogrammeerd script zijn of bij complexere vragen een fysiek persoon. De patiënt logt in de app van de eCoach en krijgt zo toegang tot de informatie. Via dit soort apps kan de patiënt -bij complexere zorgvragen- ook communiceren met de zorgverlener. De gebruiksfrequentie verschilt tussen een paar keer per dag tot een keer per week (mede afhankelijk van de fase van het zorgpad van de patiënt).

Casus: eCoaches	
AVG-rol van de leverancier	**Betrouwbaarheidsniveau**
Verwerker van de zorgaanbieder	- het gaat om specifieke informatie die aansluit bij het ziektebeeld en de fase waarin de patiënt zich bevindt in het kader van de behandeling. Het gaat dus niet om algemene, niet op de individuele patiënt gericht informatie. Tevens kan gecommuniceerd worden met de zorgverlener. - de leverancier van de app werkt onder verantwoordelijkheid van de zorgaanbieder. - de gegevens die aan de patiënt worden verstrekt door een script of fysieke persoon (informatie over de ziekte) en de communicatie met de zorgverlener vallen onder het medisch beroepsgeheim. Deels zal dit ook moeten worden opgenomen in het medisch dossier. - Er kan sprake zijn van het verwerken van het BSN in combinatie met andere gegevens. **Betrouwbaarheidsniveau hoog is vereist**
Verwerkingsverantwoordelijke	Het zou zo kunnen zijn dat een patiënt zelf een app heeft aangeschaft waar informatie kan worden verkregen over het ziektebeeld en waar bijvoorbeeld online vragenlijsten worden aangeboden aan de hand waarvan de patiënt

	zelf een diagnose kan stellen. Er wordt geen advies gegeven door de leverancier van de app n.a.v. de vragenlijsten. Dan is sprake van het verwerken van gezondheidsgegevens die niet onder het medisch beroepsgeheim vallen. **Minimaal betrouwbaarheidsniveau substantieel is vereist.** Uiteraard geldt dan dat het vervolgens voor het toegang krijgen tot de gegevens door de zorgverlener andere voorwaarden kunnen gelden.

3.2.4 Beeldbellen

Via de beeldbel-apps logt de patiënt in en kan de patiënt via die weg digitaal in contact komen met de zorgverlener. De gebruiksfrequentie kan oplopen tot een paar keer per dag.

Volgens de KNMG handreiking videoconsulten[28] is een videoconsult een consult waarbij de arts op afstand zorgt verleent aan de patiënt via een directe ('live') videoverbinding. Onder 'videoconsult' vallen verschillende begrippen zoals ook videobellen, beeldbellen, e-consult, beeldconsult of screen-to-screenconsult.

De KNMG adviseert in elk geval om een veilige en gecertificeerde applicatie te gebruiken. Daarbij valt te denken aan toepassingen die speciaal voor de zorg ontwikkeld zijn. De Autoriteit Persoonsgegevens heeft een keuzehulp ontwikkeld waarmee verschillende applicaties op privacyaspecten worden vergeleken.[29] LHV, InEen en NHG hebben ook een overzicht gemaakt van bestaande applicaties waarbij o.a. gekeken is of ze ontworpen zijn voor de zorg.[30]

Casus: beeldbellen	
AVG-rol van de leverancier	**Betrouwbaarheidsniveau**
Verwerker van de zorgaanbieder	De inschatting van het vereiste betrouwbaarheidsniveau voor inloggen kan afhankelijk zijn van hoe de beeldbel-app in het proces van de zorgaanbieder is ingebed. Bij beeldbellen is sprake van een online behandeling van de patiënt, alles wat wordt uitgewisseld valt daarmee onder het medisch beroepsgeheim. De vraag is meer of inloggen in alle gevallen op niveau hoog vereist is aangezien de zorgverlener de patiënt kan zien en dus zelf kan identificeren/authenticeren.

[28] KNMG, 'Alles wat u moet weten over videoconsulten met patiënten', 27 september 2021.

[29] Autoriteit Persoonsgegevens Autoriteit Persoonsgegevens, 'Keuzehulp privacy bij videobel-apps', 15 april 2020.

[30] LHV, 'Beeldbellen en videoconsult'.

	- Als de app via het portaal van de zorgaanbieder moet worden benaderd en de patiënt daarmee toegang krijgt tot medische gegevens geldt dat **betrouwbaarheidsniveau hoog** is vereist. - Als het gaat om een app die apart te benaderen is, zou afhankelijk van het proces dat de zorgverlener volgt een lager betrouwbaarheidsniveau mogelijk zijn.
Verwerkingsverantwoordelijke	Er zijn ook zakelijke beeldbeltoepassingen. Die worden specifiek voor de zakelijke markt, al dan niet gratis, aangeboden door commerciële bedrijven. Deze zakelijke toepassingen zijn niet specifiek ontwikkeld voor de zorg. De KNMG raadt aan om dan in elk geval te werken met betaalde opties zodat er afspraken kunnen worden gemaakt over wat er met de data gebeurt.[31] Indien deze toepassingen grootschalig bijzondere persoonsgegevens verwerken, is **minimaal betrouwbaarheidsniveau substantieel vereist.**

3.2.5 Digitale asynchrone communicatie

Bij asynchrone digitale communicatie wordt gebruik gemaakt van apps waarmee beveiligde berichten tussen zorgverlener en patiënt uitgewisseld kunnen worden. De patiënt stelt bij voorbeeld een vraag, de zorgaanbieder beantwoord deze op een later moment. De gebruiksfrequentie kan oplopen tot meerdere keren per dag.

Casus: digitale asynchrone communicatie	
AVG-rol van de leverancier	**Betrouwbaarheidsniveau**
Verwerker van de zorgaanbieder	- Er is sprake van communicatie tussen de zorgverlener en de patiënt in het kader van de behandeling - de leverancier werkt onder verantwoordelijkheid van de zorgaanbieder. - de gegevens die door de toepassing worden ingevoerd en verstuurd

[31] KNMG-richtlijn: Omgaan met medische gegevens, november 2022, p. 55.

	vallen onder het medisch beroepsgeheim. - Er kan sprake zijn van het verwerken van het BSN in combinatie met andere gegevens. **Betrouwbaarheidsniveau hoog is vereist**
Verwerkingsverantwoordelijke	De patiënt zou een app kunnen gebruiken die niet door de zorgaanbieder is aangeschaft en voorgeschreven. Indien deze toepassingen grootschalig bijzondere persoonsgegevens verwerken, is **minimaal betrouwbaarheidsniveau substantieel vereist.** De leverancier kan dan niet meeliften op de grondslagen voor verwerking van de zorgaanbieder. BSN kan niet verwerkt worden door de leverancier.

3.2.6 Digitale vragenlijsten

Digitale vragenlijsten van de zorgaanbieder worden via een app of cliëntenportaal ingevuld door de patiënt en verstuurd naar de zorgverlener. De zorgverlener kan deze vragenlijsten inzien in een cliëntenportaal of via een directe koppeling in het EPD (HL7-koppeling).

Casus: digitale vragenlijsten	
AVG-rol van de leverancier	**Betrouwbaarheidsniveau**
Verwerker van de zorgaanbieder	- het gaat om specifieke informatie over de patiënt en het ziektebeeld. Het gaat dus niet om algemene, niet op de individuele patiënt gericht informatie. De informatie wordt verzameld in het kader van de behandeling. - de leverancier van de app werkt onder verantwoordelijkheid van de zorgaanbieder. - De gegevens vallen onder het medisch beroepsgeheim en worden opgenomen in het medische dossier. - Er kan sprake zijn van het verwerken van het BSN in combinatie met andere gegevens. **Betrouwbaarheidsniveau hoog is vereist**
Verwerkingsverantwoordelijke	Het zou zo kunnen zijn dat een patiënt zelf een app gebruikt waar online vragenlijsten worden aangeboden. Dan is sprake van het verwerken van gezondheidsgegevens die niet onder het

	medisch beroepsgeheim vallen. **Minimaal betrouwbaarheidsniveau substantieel is vereist.** Uiteraard geldt dat vervolgens voor het toegang verkrijgen tot de gegevens door de zorgverlener andere voorwaarden kunnen gelden.

3.2.7 Cliëntenportaal

E-health portaal/ cliëntportaal GGZ

In de GGZ vindt een belangrijk deel van de behandeling plaats in een e-health portaal en/of cliëntportaal. Bij de meeste portalen loggen cliënten in via een multi-factor authenticatie. In het portaal gaat een cliënt aan de slag met psycho-educatie, online behandelmodules, dagboeken, vragenlijsten en de meeste portalen hebben de mogelijkheid om te beeldbellen met de behandelaar.

Casus: cliëntenportaal GGZ	
AVG-rol	**Betrouwbaarheidsniveau**
Verwerker van de zorgaanbieder	Onduidelijk is of de cliënt in dit geval ook toegang krijgt tot (een deel van) het medisch dossier via het portaal. Los daarvan: - Een belangrijk deel van de behandeling vindt plaats via het portaal. De cliënt voert allerlei gegevens in over het eigen ziektebeeld (in de vorm van dagboeken, behandelmodules, vragenlijsten etc). - de leverancier van het portaal werkt onder verantwoordelijkheid van de zorgaanbieder. - de gegevens die door de patiënt worden ingevoerd en verstuurd vallen onder het medisch beroepsgeheim. **Betrouwbaarheidsniveau hoog is vereist**
Zelfstandig verwerkingsverantwoordelijke	Het is onwaarschijnlijk dat een cliëntenportaal niet onder de verwerkingsverantwoordelijkheid van de zorgaanbieder zou vallen.

3.2.8 Mobiele apps

In toenemende mate maken GGZ cliënten gebruik van apps en specifieke e-health applicaties. Denk aan dagboeken, stress reductie apps, VR brillen, zorgrobotica, etc. Zie voor de analyse van de vereiste betrouwbaarheidsniveaus de bovenstaande casus ‘Thuis behandelen’.

4. Oplossingsrichtingen

4.1 Inleiding

Op basis van de gehouden interviews, literatuurstudie en onze eigen kennis en ervaring komen we tot enkele oplossingsrichtingen. Bij de indeling hiervan hebben we nadrukkelijk rekening gehouden met de tijdslijnen van het IZA m.b.t. hybride zorg. De oplossingsrichtingen zijn verdeeld in twee categorieën:

1. oplossingsrichtingen op korte termijn; en
2. oplossingsrichtingen op langere termijn.

Deze oplossingsrichtingen vullen elkaar aan en kunnen naast elkaar worden geïmplementeerd.

4.2 Oplossingsrichtingen op korte termijn

Het betrouwbaarheidsniveau eIDAS Hoog is momenteel nog niet breed beschikbaar voor patiënten/burgers. BZK zal het in de komende jaren nader ontwikkelen op basis van het Stelsel Toegang van BZK. Dit stelsel is dus nog niet gereed. Er zijn wel gebruiksvriendelijke private middelen gebaseerd op de meest moderne (mobiele) technologieën op betrouwbaarheidsniveau hoog beschikbaar, maar deze zijn nog niet erkend onder de Wdo. Bovendien is daar nog geen financiering voor, waardoor deze middelen (nog) niet breed beschikbaar zijn. Ook voor nutsmiddelen is nog geen Wdo-erkenning en publieke financiering beschikbaar.

Het lijkt daarmee onwaarschijnlijk dat de acceptatieplicht van erkende en toegelaten middelen vanuit de Wdo op korte termijn in werking zal treden.

Tegelijkertijd hebben de geïnterviewden aangegeven dat zij belang hechten aan een balans tussen vertrouwen en gebruiksvriendelijkheid. Om die reden lijkt het niet raadzaam om veel zorgaanbieders op betrouwbaarheidsniveau laag te houden totdat BZK het Stelsel Toegang gereed heeft voor eIDAS Hoog en de bijbehorende middelen breed beschikbaar zijn. Vandaar dat als eerste oplossingsrichting het gefaseerd invoeren van het betrouwbaarheidsniveau substantieel wordt uitgewerkt, naast het opschalen van bestaande ondersteuningsvormen, het combineren van technologische en organisatorische beveiligingsmaatregelen, het aanpassen van wet- en regelgeving en de communicatie van alle authenticatiemogelijkheden.

4.2.1 Gefaseerd invoeren van betrouwbaarheidsniveau substantieel

Als het gaat om betrouwbaarheidsniveau substantieel is DigiD Substantieel het meest breed beschikbare middel voor burgers. Ook hier geldt dat er private en nutsmiddelen zijn op betrouwbaarheidsniveau substantieel, maar dat deze door gebrek aan erkenning en financiering (nog) niet breed beschikbaar zijn.

In aanvulling op de huidige activiteiten van VWS zou VWS de zorgsector meer kunnen faciliteren om gefaseerd opschaling naar betrouwbaarheidsniveau substantieel mogelijk te maken. Van de zijde van VWS vergt dit tenminste een plan van aanpak hoe te komen tot brede, gebruiksvriendelijke beschikbaarheid, rekening houdend met inclusie van mensen die niet zelf digitaal vaardig zijn. Bij dit

plan van aanpak kan de ToegangVerleningService ("**TVS**" – ontsluitende dienst) worden ingezet aangezien een toenemend deel van de zorgaanbieders al op TVS is aangesloten.

Veel van de geïnterviewden zien minder problemen wat betreft gebruiksvriendelijkheid op betrouwbaarheidsniveau substantieel en zien tegelijkertijd wel een betere borging van vertrouwde omgang met gezondheidsgegevens dan bij het op dit moment veelal nog gehanteerde betrouwbaarheidsniveau laag. Tijdens de coronapandemie hebben veel burgers inmiddels al kennisgemaakt met betrouwbaarheidsniveau substantieel. Overigens is er ook vanuit juridische optiek ruimte om fasering toe te staan, door te beginnen met een betrouwbaarheidsniveau één niveau lager dan vereist. In artikel 6, vierde lid, Wdo juncto artikel 6, eerste lid, Regeling betrouwbaarheidsniveaus is de mogelijkheid opgenomen om tijdelijk een lager betrouwbaarheidsniveau toe te staan.

Om tot een gefaseerde aanpak te komen zijn er volgens de geïnterviewden diverse strategieën.

Ten eerste conform de adoptie-theorie: waarbij een onderscheid wordt gemaakt tussen de voorlopers, de hoofdgroep en de achterblijvers.

Ten tweede gericht op maximale gebruiksmogelijkheden: in dat geval wordt bij de grote groep begonnen en in eerste instantie niet de uitzonderingsgevallen. Het is de vraag in hoeverre deze door bedrijven vaak gehanteerde strategie ook in het publieke domein gewenst is, waar inclusie een belangrijke voorwaarde is.

Ten derde zou met het oog op die inclusie juist een gefaseerde aanpak rekening kunnen houden met speciale doelgroepen.

De suggestie is gedaan om bij de gefaseerde invoering van betrouwbaarheidsniveaus uit te gaan van een zogenaamde 'fuik-methode': Als een persoon eenmaal op een hoger betrouwbaarheidsniveau geïdentificeerd is, mag die persoon niet langer met middelen met een lager betrouwbaarheidsniveau werken.

4.2.2 Opschalen van bestaande ondersteuningsvormen

Een tweede oplossingsrichting is het opschalen van al bestaande ondersteuningsvormen voor zowel patiënten/burgers als zorgverleners. Dit is niet alleen ter ondersteuning van het inloggen op een hoger betrouwbaarheidsniveau, maar ook voor het gebruik van hybride zorg in den brede.

Voor patiënten kan worden gedacht aan het opschalen van de al bestaande zorgbalies bij bijvoorbeeld ziekenhuizen. Ook bibliotheken bieden op dit moment al hulp bij het gebruik van DigiD en het gebruik van bijvoorbeeld BeterDichtbij. Welzijnsorganisaties, de cliëntenhelpdeks bij GGZ en de Helpdesk Digitale Zorg bieden aan patiënten en burgers ook ondersteuning bij betrouwbaar inloggen bij hybride zorg. De ondersteuningsvormen kunnen tot op bepaalde hoogte ondersteuningen bieden, omdat zij beperkte mogelijkheden en bevoegdheden hebben. Om de IZA-doelstellingen te halen zullen deze bestaande ondersteuningsvormen flink moeten worden

opgeschaald en zal moeten worden onderzocht of meer mogelijkheden en bevoegdheden aan deze ondersteuningsvormen kan worden gegeven.[32]

Daarnaast is ook aandacht nodig voor de ondersteuning van zorgverleners. Veel zorgverleners krijgen van hun patiënten de vraag hoe ze om moeten gaan met de toepassingen die worden ingezet voor hybride zorg. Betere ondersteuning van zorgverleners kan hen helpen om patiënten/burgers op een hoger betrouwbaarheidsniveau geauthentiseerd te krijgen. Gedacht kan worden aan digicoaches en I-nurses die zo hier en daar al actief zijn.

Een digicoach is een medewerker (zorgprofessional, servicedeskmedewerker, fysiotherapeut enz.), met meer gevoel voor digitale ontwikkeling dan de collega's, die met uren in staat gesteld wordt om nabije collega's met raad en daad op de werkvloer terzijde te staan bij het gebruik van digitale middelen en de daarvoor benodigde vaardigheden. Hij/zij coacht collega's zodat zij zo zelfstandig mogelijk digitaal kunnen werken.

Een I-nurse is een zorgprofessional die de rol vervult van innovatieambassadeur. Dat is iemand die bijvoorbeeld 2-3 dagen is vrijgesteld om op zoek te gaan naar e-healthinnovaties en te helpen bij de invoering. De I-nurse heeft vanuit een verbindende rol veel contact met de innovatie-afdeling, de digicoach, medewerkers en cliënten, maar een I-nurse werkt voor het grootste deel van de tijd als zorgmedewerker.[33]

De ondersteuningsvormen dragen er aan bij dat het voor zowel patiënten als zorgverleners altijd mogelijk is om een natuurlijke persoon te spreken die hen kan helpen bij betrouwbaar inloggen bij hybride zorg.

4.2.3 Technologische oplossingen die al kunnen en zijn toegestaan

Zowel vanuit beveiligingsoptiek als voor een betere gebruiksvriendelijkheid, wordt als belangrijkste oplossingsrichting *'Mobile First'* genoemd. Met *Mobile First* wordt bedoeld dat voor *verreweg de meeste toepassingen* (First) een smartphone[34] (i.e. slimme telefoon) gebruikt zal worden, omdat de meeste mensen een smartphone hebben en deze veel (dagelijks) gebruiken. Ook bij nieuwe toepassingen, zoals een smartwatch gebruikt men feitelijk een smartphone. Daarmee is de smartphone een spin in het web. Toch is de smartphone niet de enige oplossing, omdat niet iedereen een smartphone heeft, kan of wil gebruiken dan wel de betreffende taal verstaat.

Gebruiksvriendelijke, private middelen met mobiele technologie zijn op dit moment vooral gericht op betrouwbaarheidsniveau hoog. Daarover gaat paragraaf 4.3.2. De vraag is in hoeverre deze

[32] Zie ook Algemene Rekenkamer, 'Digitale identiteit vraagt veel van DigiD en eHerkenning', maart 2023, p. 6 onder Ondersteuning niet-digivaardigen en burgers met complexe problematiek kan beter.

[33] Digivaardigheid in de zorg, 'De digicoach en de I-nurse, Samen werken ze aan een digitale toekomst!'.

[34] *"A smartphone is a cellular telephone with an integrated computer and other features not originally associated with telephones, such as an operating system (OS), web browsing and the ability to run software applications. Smartphones are used by consumers and as part of a person's business or work. They provide access to many mobile applications and computing functions and have become integral to everyday modern life."* Bron: Techtarget.com.

technologie ook al op betrouwbaarheidsniveau substantieel kan worden ingezet nu in de praktijk vooral DigiD Substantieel beschikbaar is (zonder deze moderne technologie).

In combinatie met mobiele technologie is voor de eerste keer inloggen door gebruik te maken van een video/filmpje een mogelijke oplossing.

Naast mobiele technologie kan ook biometrie helpen bij gebruiksvriendelijkheid. Biometrische identificatie is onder voorwaarden al toegestaan en eventueel ook bruikbaar op betrouwbaarheidsniveau substantieel. Voor biometrische authenticatie is nog geen grondslag in de zorg en in de Conceptregeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo ("**Conceptregeling identificatiemiddelen**") wordt biometrische authenticatie zelfs verboden. Met het oog op gebruiksvriendelijkheid zou onderzocht kunnen worden of biometrie op voldoende betrouwbare wijze kan worden ingezet en de Conceptregeling identificatiemiddelen aangepast dient te worden. Hierbij moet een eenduidig normenkader worden ontwikkeld waarbij antwoord wordt gegeven op o.a. de volgende vragen:

1. Welke betrouwbaarheid moet een biometrische authenticatie-oplossing hebben om in aanmerking te komen voor betrouwbaarheidsniveau substantieel of hoog?
2. Waaraan dient de beveiliging van de biometrische oplossing te voldoen in het geval van aanvallers met een gemiddeld of hoog aanvalspotentieel?
3. Zijn certificeringen wenselijk en praktisch te handhaven?[35]

4.2.4 Combinatie van technische en organisatorische beveiligingsmaatregelen

Bij de vierde oplossingsrichting gaat het om een combinatie van technische en organisatorische maatregelen.

De Wdo, de Regeling betrouwbaarheidsniveaus[36] en de AVG[37] bieden de mogelijkheid om door een combinatie van technische en organisatorische beveiligingsmaatregelen (zoals logging, controle op de logging en autorisatiebeheer) [38] een lager betrouwbaarheidsniveau te mogen gebruiken. Door verschillende maatregelen te combineren op een wijze dat zij elkaar ondersteunen en op elkaar aansluiten, kan een hoger betrouwbaarheidsniveau worden bereikt.

[35] Zie ook: InnoValor (B. Hulsebosch, O. Kulyk & H. de Bos), 'Biometrie voor identiteitsverificatie: Verkenning van de mogelijkheden', 20 januari 2020, par. 5.4.

[36] Zie artikel 6 Wdo juncto artikel 3, eerste lid, Regeling betrouwbaarheidsniveaus.

[37] Zie artikelen 24, 25 en 32 AVG.

[38] Zie ook Autoriteit Persoonsgegevens, brief aan GGD GHOR Nederland, 8 november 2021, p. 2.

In artikel 32 van de AVG wordt een aantal voorbeelden gegeven van passende technische en organisatorische maatregelen. Het gaat bijvoorbeeld om pseudonimisering,[39] versleuteling en testprocedures.[40]

Bij technische beveiligingsmaatregelen kan gedacht worden aan:

- logische en fysieke (toegangs)beveiliging en beveiliging van apparatuur. Denk niet alleen aan kluizen en portiers, maar ook aan firewalls, netwerksegregatie (scheiden van netwerken), autorisatie (welke medewerker heeft toegang tot wat) en accounts aan 1 persoon koppelen (zodat niet meerdere mensen hetzelfde account kunnen gebruiken);
- technisch beheer van de (zo beperkt mogelijke) autorisaties en logbestanden bijhouden;
- beheer van technische kwetsbaarheden ('patch management');
- software up-to-date houden, zoals browsers, virusscanners en besturingssystemen;
- back-ups maken waarmee u de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig kunt herstellen. Overwogen moeten worden of dubbele systemen nodig zijn, zodat het geheel goed blijft functioneren wanneer een onderdeel uitvalt;
- verouderde gegevens automatisch verwijderen;
- gegevens versleutelen (encryptie);
- hashing[41] gebruiken als methode om persoonsgegevens te pseudonimiseren; en
- minder gegevens op de servers verwerken en meer gegevensverwerkingen laten plaatsvinden op de apparatuur van de gebruiker zelf, zoals een smartphone.

Bij organisatorische beveiligingsmaatregelen kan gedacht worden aan:

- mensen verantwoordelijkheden toewijzen voor informatiebeveiliging;
- beveiligingsbewustzijn vergroten bij bestaande en nieuwe medewerkers;
- procedures opstellen om op gezette tijdstippen de beveiligingsmaatregelen te testen, te beoordelen, te evalueren en eventueel aan te scherpen;
- regelmatig de logbestanden controleren;
- een protocol opstellen voor de afhandeling van datalekken en beveiligingsincidenten;
- geheimhoudingsovereenkomsten en verwerkersovereenkomsten afsluiten;
- regelmatig beoordelen of dezelfde doelen kunnen worden behaald met minder persoonsgegevens;
- minder mensen in de organisatie toegang geven tot persoonsgegevens; en

[39] Pseudonimisering is het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. Zie artikel 4, vijfde lid, AVG.

[40] Zie ook artikelen 25 en 89 AVG.

[41] Hashing is een methode om persoonsgegevens te pseudonimiseren. Daardoor wordt het moeilijker om deze gegevens te herleiden naar personen. Hashing is een beveiligingsmaatregel en leidt niet tot anonimisering.

- per verwerking het besluitvormingsproces en de achterliggende overwegingen vastleggen.[42]

In dit kader kan ook aangesloten worden bij de regels die voortvloeien uit NEN 7510 voor wat betreft informatiebeveiliging in de zorg. Het gaat hierbij o.a. om regels m.b.t. toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging van de bedrijfsvoering en communicatiebeveiliging.

VWS werkt op dit moment aan een landelijk vertrouwensstelsel waarbij naast technische en organisatorische maatregelen ook rekening wordt gehouden met juridische maatregelen, beveiligingsnormen, betere communicatie en bijbehorende toezicht en handhaving. Door aan te sluiten bij het landelijk vertrouwensstelsel kan voor (delen van) de zorgsector mogelijk het betrouwbaarheidsniveau substantieel worden bepleit in plaats van hoog en in sommige gevallen betrouwbaarheidsniveau laag in plaats van substantieel voor tenminste de overgangsperiode van de komende jaren.

Wel moet worden vastgesteld onder welke omstandigheden een lager betrouwbaarheidsniveau zou kunnen en mogen worden gebruikt.[43]

4.2.5 Aanpassen wet- en regelgeving

Logius-regels

In de zorgpraktijk blijkt dat de regels van Logius voor het aansluiten en gebruik van DigiD tot problemen leiden. Het is de vraag of die regels noodzakelijk zijn gelet op de bestaande wet- en regelgeving en waar ruimte bestaat om af te wijken. Uitgezocht dient te worden in hoeverre de regels van Logius met inachtneming van wet- en regelgeving aangepast kunnen worden in de zorgpraktijk. Uiteindelijk zal dit input leveren voor de ‘aansluitvoorwaarden’ die zullen gaan gelden voor het aansluiten op het Stelsel Toegang (deze vervangen de voorwaarden voor aansluiting op DigiD) en die worden vastgelegd in een ministeriële regeling.

Voorbeelden van regels van Logius die onderzocht kunnen worden zijn de 15-minuten regel bij inactiviteit bij SSO en het aansluiten per domein (zie par. 2.3). Daarnaast zal met BZK en Logius gesproken dienen te worden in hoeverre zij rekening kunnen houden met de toenemende trend van netwerkzorg en ketenzorg.

Bovendien zou bestaande algemene wetgeving in meer concrete normen kunnen worden vertaald, zodat leveranciers weten waar ze aan toe zijn. Dit kan bijvoorbeeld door een NEN-norm of andere normering waarin staat hoe betrouwbaarheidsniveau substantieel of hoog bereikt kan worden door een combinatie van beveiligingsmaatregelen.

Voor de volledigheid merken we op dat enkele geïnterviewden in de wetgeving een uitzonderingspositie voor zichzelf zouden willen zien, waardoor zij bijvoorbeeld een publieke status krijgen.

[42] Autoriteit Persoonsgegevens, ‘Voorbeelden van beveiligingsmaatregelen’.

[43] MvT: Tweede Kamer, vergaderjaar 2017–2018, 34 972, nr. 3.

Biometrie

In artikel 2.13 van de Conceptregeling identificatiemiddelen is een verbod opgenomen voor een identificatiemiddel waarbij authenticatie plaatsvindt met gebruik van biometrische gegevens. Voor een nadere uitleg wordt verwezen naar Bijlage 1: Juridisch kader vereiste betrouwbaarheidsniveau inlogmiddelen digitale diensten. Op zich is dat verbod te begrijpen omdat alleen biometrische authenticatie onvoldoende betrouwbaar is. Om deze reden is als aanvulling op biometrische authenticatie ook een pincode vanuit veiligheidsoptiek noodzakelijk.

Denkend in termen van oplossingen, zou door VWS samen met BZK onderzocht kunnen worden onder welke voorwaarden het gebruik van biometrie voor authenticatie wel toegestaan zou kunnen worden. Voor de overheid geldt dat hiervoor een wettelijke grondslag geregeld moet worden.

VWS zal dan, met behulp van de zorgsector en de bijbehorende leveranciers, wel met goede argumenten en benodigde waarborgen moeten komen richting BZK. Bovendien mogen genotificeerde eIDAS-middelen die door Nederlandse dienstverleners geaccepteerd moeten worden wel gebruik maken van biometrie als authenticatiefactor.[44]

4.2.6 Communicatie van alle authenticatiemogelijkheden

Op dit moment kennen de meeste burgers eigenlijk alleen DigiD.[45] Er zijn private middelen, bijvoorbeeld van het afsprakenstelsel eHerkenning en iDIN vanuit de financiële wereld, die een substantieel of hoog betrouwbaarheidsniveau kunnen bieden op een meer gebruiksvriendelijke wijze dan het huidige DigiD. Bij de communicatie (door BZK) over de Wdo verdient het aanbeveling dat naast DigiD ook private middelen bekend worden gemaakt. Overigens zou dit niet alleen voor private middelen moeten gelden, maar ook voor nuts-toepassingen, zoals op dit moment bijvoorbeeld Yivi aangeeft te zijn.

4.3 Oplossingsrichtingen op langere termijn

Bovenstaande oplossingsrichtingen zijn voor de korte termijn. Op korte termijn is betrouwbaarheidsniveau hoog nog niet te realiseren. Op langere termijn zal voor hybride zorg in verreweg de meeste gevallen betrouwbaarheidsniveau hoog vereist zijn zodra dit praktisch op brede schaal mogelijk wordt. Hierna volgen oplossingsrichtingen voor de langere termijn.

---

[44] Zie ook Conceptbrief van eHerkenning, 2 december 2022, m.b.t. artikel 2.13 van de Conceptregeling identificatiemiddelen: "*Het is onduidelijk waarom het gebruik van biometrie als authenticatie-factor expliciet wordt uitgesloten (art. 2.13). Wij zien dit als een gemiste kans als deze keuze overeind blijft. Het level playing field wordt hierdoor scheef getrokken. Elders in de EU mag dit namelijk wel. Genotificeerde eIDAS-middelen die door Nederlandse dienstverleners geaccepteerd móeten worden mogen wél gebruik maken van biometrie als authenticatiefactor.*"

[45] Kamerstukken II 2014/15, 34059, nr. 6: "*Voor burgers is het huidige beschikbare authenticatiemiddel inderdaad DigiD. Er zijn voor DigiD twee betrouwbaarheidsniveaus beschikbaar: laag en midden.*"

4.3.1 Gefaseerd invoeren van betrouwbaarheidsniveau hoog

Op dit moment leveren bijna alle zorgaanbieders diensten op betrouwbaarheidsniveau laag. Alle geïnterviewden zien voor het overgrote deel van de digitale dienstverlening in de zorg uiteindelijk betrouwbaarheidsniveau eIDAS Hoog als vereist en gewenst voor een vertrouwde omgang met gezondheidsgegevens.

Hoewel het op dit moment ontbreken van breed beschikbare middelen op niveau eIDAS Hoog risico's met zich meebrengt om te komen tot vertrouwde digitale dienstverlening in de zorg, met bijvoorbeeld meer kans op datalekken en cybercrime, is dit tegelijkertijd een opluchting voor degenen die bang zijn dat de doelstellingen uit het IZA voor hybride zorg niet gehaald kunnen worden als gevolg van de huidige gebruiksonvriendelijkheid van DigiD Hoog. Mede gelet op het feit dat betrouwbaarheidsniveau hoog formeel op grond van de eIDAS-verordening en de Wdo wel verplicht is (zie het juridisch kader in Bijlage 1) en de AP de afwezigheid hiervan gedoogt totdat middelen op het betrouwbaarheidsniveau hoog wel voldoende breed beschikbaar zijn, is het van belang om bij BZK duidelijkheid te krijgen over de planning om te komen tot breed beschikbare middelen op betrouwbaarheidsniveau hoog. Tot op heden is deze duidelijkheid er nog niet terwijl de Wdo wel al in werking is. Het is urgent dat die duidelijkheid er op korte termijn komt.

4.3.2 Technologische oplossingen: Mobile First, biometrie en Wallet

Mobile First (en biometrie)

Er zijn toepassingen op de markt met betrouwbaarheidsniveau hoog, waarbij men na eenmalige on boarding voor authenticatie naast een smartphone bijvoorbeeld alleen een QR-code nodig heeft. Dat is veel eenvoudiger dan steeds het identiteitsbewijs te moeten gebruiken. In plaats van QR-code kan ook gebruik worden gemaakt van SMS.

In dit kader wordt ook wel gesproken van zogenaamde passkeys. Passkeys zijn een soort digitale sleutels die veilig op een apparaat worden bewaard en waar een persoon alleen met zijn vingerafdruk, gezichtsherkenning of een pincode bij kan. Passkeys zorgen ervoor dat oplichting via phishing (nepwebsites) vrijwel onmogelijk is. Deze digitale sleutel wordt per website aangemaakt en werk alleen met die website. Het tweede voordeel zou zijn dat passkeys veel lastiger worden gehackt.[46]

Met name het gebruiken van de beveiligingsopties die een smartphone op het gebied van biometrie, zoals extra beveiliging door gebruik te maken van een vingerafdruk of gezichtsherkenning, wordt als oplossing gezien. De uitdaging is wel dat het verboden is om biometrische persoonsgegevens te verwerken, tenzij er een wettelijke uitzondering geldt.[47] Het gebruik van biometrie als authenticatie-factor wordt in de artikel 2.13 van *conceptregeling* nadere eisen toelating identificatiemiddelen Wdo uitgesloten.

[46] RTL Nieuws (D. Verlaan), 'Met de nieuwe passkeys mag je jouw wachtwoorden (eindelijk) vergeten', 28 oktober 2023.

[47] Zie artikel 9 AVG.

Volgens de AP zijn de twee meest voor de hand liggende uitzonderingen op het verbod voor het gebruiken van gezichtsherkenning dat:

1. gezichtsherkenning noodzakelijk is voor authenticatie of beveiliging;
2. de verwerkingsverantwoordelijke uitdrukkelijke toestemming van de betrokkene heeft gekregen (om te filmen).[48]

Denkend in termen van oplossingen, zou voor gebruik van biometrie voor authenticatie door VWS samen met BZK onderzocht kunnen worden onder welke voorwaarden het gebruik van biometrie voor authenticatie op een betrouwbare wijze toegestaan zou kunnen worden, zoals bijvoorbeeld voor de banken Europees al is geregeld. Bovendien mogen genotificeerde eIDAS-middelen die door Nederlandse dienstverleners geaccepteerd moeten worden wel gebruik maken van biometrie als authenticatiefactor.[49]

Naast biometrische authenticatie is het bij een mobiele telefoon/smartphone mogelijk om een code te vinden in de ene app en vervolgens de authenticatie zelf plaats te laten vinden via een andere app.

De uitdaging bij het gebruiken van smartphones is dat bij smartphones sprake is van een beperkte houdbaarheid in tijd voordat het vervangen moet worden (met name bij smartphones die het Android-systeem gebruiken). De ontwikkeling van de smartphones is afhankelijk van de ontwikkelaar en het besturingssysteem dat wordt gebruikt.

Naast het gebruiken van een smartphone wordt in toenemende mate ook gebruik gemaakt van intelligent devices die ook de applicaties van smartphones hebben.

Wallet op basis van eIDAS 2.0

Bij de herziene eIDAS-verordening ("**eIDAS 2.0**") zal elke lidstaat de plicht krijgen om ten minste een (1) European Digital Identity Wallet ("**Wallet**") te introduceren. Een wallet, of digitale portemonnee, is een applicatie waarin een burger of onderneming zijn identiteitsgegevens en officiële documenten elektronisch kan opslaan en beheren. Ook kan de burger zichzelf er digitaal mee identificeren en online een handtekening zetten. Enkele grote merken zoals Apple en Google bieden

[48] Autoriteit Persoonsgegevens, 'Gezichtsherkenning'.

[49] Zie ook Conceptbrief van eHerkenning, 2 december 2022, m.b.t. artikel 2.13 van de Conceptregeling identificatiemiddelen: "*Het is onduidelijk waarom het gebruik van biometrie als authenticatie-factor expliciet wordt uitgesloten (art. 2.13). Wij zien dit als een gemiste kans als deze keuze overeind blijft. Het level playing field wordt hierdoor scheef getrokken. Elders in de EU mag dit namelijk wel. Genotificeerde eIDAS-middelen die door Nederlandse dienstverleners geaccepteerd móeten worden mogen wél gebruik maken van biometrie als authenticatiefactor.*"

ook een vorm van wallet aan.[50] Feitelijk maken o.a. Yivi[51], KPN[52], Digidentity[53] en Cleverbase /Vidua[54] al gebruik van een wallet.

De Wallet dient burgers en bedrijven die dit willen, de mogelijkheid te bieden om onder een hoog beveiligingsniveau hun elektronische identiteit en daaraan gelinkte attributen, zoals kwalificaties, bevoegdheden en digitale documenten, zelf ter beschikking te stellen in online en offline transacties, in het publieke en het private domein. eIDAS 2.0 bepaalt dat het gebruik van de Wallet gratis ("free of charge") moet zijn voor natuurlijke personen. [55][56]

Wanneer een burger als Nederlandse burger in de toekomst een wallet wil gebruiken, installeert de burger deze als app op zijn telefoon of een ander (draagbaar) apparaat. De burger vult deze met door de overheid gewaarmerkte identiteitsgegevens. Vanaf dan kan de burger zichzelf online identificeren, bij alle overheidsdiensten in de lidstaten van de EU, bij private dienstverleners, zoals banken en verzekeraars, en bij grote online platforms. Ook kan de burger extra geverifieerde gegevens toevoegen aan de wallet, uit zowel publieke als private bronnen. Denk daarbij aan het rijbewijs, diploma's en certificaten, beroepskwalificaties, inkomensgegevens, maar mogelijk ook betaalpassen, de OV-chipkaart en festivaltickets. [57]

Daar waar de Wdo-middelen nog te weinig soelaas bieden, zou de Wallet een alternatief kunnen zijn. Om te zorgen dat alle burgers en bedrijven, volgens de doelstelling van eIDAS 2.0, in 2025 gebruik kunnen maken van een hoogwaardige wallet heeft BZK een programma ingericht dat een eerste versie van een Nederlandse open source wallet zal neerzetten. De Nederlandse open source publieke wallet is een voorbeeld wallet waaraan gewerkt wordt om de ontwikkelingen in het domein van digitale identiteit, in het bijzonder met betrekking tot de eIDAS 2.0, te beïnvloeden. Er wordt een voorbeeld wallet ontwikkeld op een wijze die past bij de publieke waarden die we in Nederland belangrijk vinden, zoals privacy, veiligheid en betrouwbaarheid. Deze activiteiten vinden plaats binnen de werkagenda "Waardegedreven digitaliseren" van BZK.[58]

---

[50] Digitale overheid, 'ID-Wallet'.

[51] Zie ook Yivi, 'Digital Identity Wallet': "Yivi is a digital wallet on your mobile phone, which you as a user fill with your digital identity and personal data".

[52] KPN, Wat is PiM?'.

[53] Zie ook Digidentity, 'De eenvoudigste en snelste manier om uw eHerkenning te regelen': "*Uw eHerkenningsaccount met de gegeven autorisatie wordt veilig opgeslagen in uw Digidentity wallet*".

[54] Vidua, 'Onbezorg online identificeren'.

[55] VNG, Analyse Samenhang: Europese digitale wetgeving fase 1 Eindrapport, p. 13-15.

[56] Zie het conceptartikel 6a lid 6 van eIDAS 2.0: *"The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high'. The use of the European Digital Identity Wallets shall be free of charge to natural persons."*

[57] Edi.pleio.nl, 'Wat is een wallet?'.

[58] Kamerstukken II 2023/24, 36410 VII, nr. 11, vraag 86.

4.3.3 Aanpassen wet- en regelgeving

Na nog uit te voeren onderzoek naar de mogelijkheden, wenselijkheid en betrouwbaarheid van biometrische authenticatie in de zorg zou op Europees niveau bepleit kunnen worden dat, onder strikte voorwaarden, net als in PSD2[59] biometrie voor authenticatie toegestaan zou kunnen worden. Daarbij is in aanvulling op biometrische authenticatie minimaal een pincode vanuit veiligheidsoptiek noodzakelijk.

[59] Gereguleerd in de regulatory technical standards over sterke cliëntauthenticatie (strong customer authentication, SCA) in aanvulling op de Payment Services Directive 2 (PSD2), middels gedelegeerde Verordening (EU) 2018/389 van 27 november 2017, PbEU 2018, L 69/23-43.

Zie M.C.A. Duijvestijn, 'Het gebruik van kunstmatige intelligentie bij de beoordeling van kredietwaardigheid van klanten in de bancaire praktijk, Brengt de AI-verordening hier verandering in?'', *MvV* 2022, nr. 9, p. 311.

Bronvermelding

Verordeningen, wetten en documentatie m.b.t. wetgevingsproces (incl. conceptwetgeving)

- **AVG**, te raadplegen via https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016R0679&qid=1685451198313.
- **Bdo**, te raadplegen via https://www.internetconsultatie.nl/digitaleoverheid/document/3439.
- **Boek 7 van het Burgerlijk Wetboek**, te raadplegen via https://wetten.overheid.nl/BWBR0005290/2023-07-01.
- **Conceptbesluit identificatiemiddelen**, te raadplegen via https://www.internetconsultatie.nl/identificatiemiddelen/document/5663.
- **Conceptregeling identificatiemiddelen** incl. toelichting, te raadplegen via https://open.overheid.nl/repository/ronl-6776536893275570966 7befed8c491ddb5cba0f9/1/pdf/concept-regeling-eisen-identificatiemiddelen-wdo.pdf
- **eIDAS 2.0** (incl. toelichting), te raadplegen via https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52021PC0281.
- **eIDAS-verordening**, te raadplegen via https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32014R0910&qid=1689941728375
- Kamerstukken II 1997/98, 25892, 3, p. 98-99, te raadplegen via https://zoek.officielebekendmakingen.nl/kst-25892-3.html.
- Kamerstukken II 2022/23, 36410, nr. 2, te raadplegen via https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/begrotingen/2023/09/19/xvi-volksgezondheid-welzijn-en-sport-rijksbegroting-2024/xvi-volksgezondheid-welzijn-en-sport-2024.pdf.
- Kamerstukken II 2023/24, 36410-VII, nr. 2, te raadplegen via https://zoek.officielebekendmakingen.nl/kst-36410-VII-2.pdf.
- Kamerstukken II 2023/24, 36410 VII, nr. 11, te raadplegen via https://zoek.officielebekendmakingen.nl/kst-36410-VII-11.pdf.
- **Regeling betrouwbaarheidsniveaus,** te raadplegen via https://wetten.overheid.nl/BWBR0048168/2023-07-01.
- **Uitvoeringsverordening** van de Commissie van 8 september tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, te raadplegen via https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32015R1502&from=EN.
- **Wabvpz**, te raadplegen via https://wetten.overheid.nl/BWBR0023864/2023-07-01.
- **Wdo**,te raadplegen via https://wetten.overheid.nl/BWBR0048156/2023-07-01.

Overige bronnen o.a. boeken, tijdschriftartikelen en (online) publicaties

- A. Hendriks, 'Het medisch beroepsgeheim. Enige actuele dilemma's', NJCM-Bulletin 2001, jrg. 26, nr. 5, te raadplegen via https://njcm.nl/wp-content/uploads/ntm/T2b_NTM2FNJCM-bull2E_010534_Final_LR.pdf.
- A.C. Hendriks, Het medisch beroepsgeheim anno 2016: gewenste en ongewenste veranderingen, Tijdschrift voor Gezondheidsschade, Milieuschade en Aansprakelijkheidsrecht 2015, afl. 4, p. 164-168, te raadplegen via https://scholarlypublications.universiteitleiden.nl/access/item%3A2857422/view.

- Algemene Rekenkamer, 'Digitale identiteit vraagt veel van DigiD en eHerkenning', maart 2023, te raadplegen via https://zoek.officielebekendmakingen.nl/blg-1082986.pdf.
- Autoriteit Persoonsgegevens Autoriteit Persoonsgegevens, 'Keuzehulp privacy bij videobel-apps', 15 april 2020, te raadplegen via https://autoriteitpersoonsgegevens.nl/actueel/keuzehulp-privacy-bij-videobel-apps.
- Autoriteit Persoonsgegevens, 'Gezichtsherkenning', te raadplegen via https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/biometrie/gezichtsherkenning#:~:text=Het%20is%20verboden%20om%20bijzondere,van%20die%20wettelijke%20uitzonderingen%20geldt.
- Autoriteit Persoonsgegevens, 'Missie, ambitie en kernwaarden', te raadplegen via https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/missie-ambitie-en-kernwaarden.
- Autoriteit Persoonsgegevens, brief aan Bestuur Nederlandse Vereniging Ziekenhuizen, 7 oktober 2016, te raadplegen via https://autoriteitpersoonsgegevens.nl/uploads/imported/brief-nvz-patientenportalen.pdf.
- Autoriteit Persoonsgegevens, brief aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, 15 oktober 2020, te raadplegen via https://autoriteitpersoonsgegevens.nl/uploads/imported/advies_regeling_betrouwbaarheidsniveaus_authenticatie_elektronische_dienstverlening.pdf.
- Autoriteit Persoonsgegevens, brief aan GGD GHOR Nederland, 8 november 2021, te raadplegen via https://www.autoriteitpersoonsgegevens.nl/uploads/imported/onderzoek_beveiliging_ggd_corona.pdf.
- Autoriteit Persoonsgegevens, brief aan het Ministerie van Volksgezondheid, Welzijn en Sport, z2018-17577, 4 oktober 2018, te raadplegen via https://autoriteitpersoonsgegevens.nl/uploads/imported/2018-10-04_brief_aan_minister_over_patientauthenticatie.pdf.
- B.W. Schermer & J. Toornstra, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', 15 april 2023, te raadplegen via https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming/Handleiding+Algemene+Verordening+Gegevensbescherming+%28AVG%29.pdf.
- Brief van BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal, 17 augustus 2022, te raadplegen via https://open.overheid.nl/documenten/ronl-e7df281c5e2045aae4dc3819da2c510030087188/pdf.
- CBP Richtsnoeren: Beveiliging van persoonsgegevens, Stc nr. 5174, 1 maart 2013, te raadplegen via https://www.autoriteitpersoonsgegevens.nl/uploads/imported/beleidsregels_beveiliging_van_persoonsgegevens.pdf.
- CBP, brief aan Flevoziekenhuis, z2005-1372, 9 mei 2006, te raadplegen via https://autoriteitpersoonsgegevens.nl/uploads/imported/z2005-1372.pdf.
- Conceptbrief van eHerkenning, 2 december 2022, m.b.t. artikel 2.13 van de Conceptregeling identificatiemiddelen, te raadplegen via https://www.eherkenning.nl/sites/default/files/2023-01/5b%20-%20Reactie%20VeHa%20op%20consultatie%20MR%20eisen%20erkenning%20private%20inlogmiddelen_def.pdf.
- Digidentity, 'De eenvoudigste en snelste manier om uw eHerkenning te regelen', te raadplegen via https://www.digidentity.eu/nl/services/digital-

identity/eherkenning?gad=1&gclid=EAIaIQobChMIk_qPnOiLggMV9Y-DBx2RPwypEAAYASAAEgJaWfD_BwE.
- Digitale Overheid, ‘eIDAS – Digitale Overheid’, te raadplegen via https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/identiteit/eidas/.
- Digitale overheid, ‘ID-Wallet’, te raadplegen via https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/identiteit/id-wallet/.
- Digitale Overheid, ‘Toelating en aansluiting van publieke & private middelen en diensten’, te raadplegen via https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/toelating-en-aansluiting-van-publieke-private-middelen-en-diensten/.
- Digitale Overheid, ‘Veelgestelde vragen over de inwerkingtreding van de Wdo’, te raadplegen via https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/veelgestelde-vragen-over-de-inwerkingtreding-van-de-wdo/.
- Digitale overheid, ‘Wet digitale overheid’, te raadplegen via https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/wetgeving/wet-digitale-overheid/.
- Digivaardigheid in de zorg, ‘De digicoach en de I-nurse, Samen werken ze aan een digitale toekomst!’, te raadplegen via https://www.digivaardigindezorg.nl/wp-content/uploads/2020/01/ECP_01272-Herdruk-I-nurse-Folder_DEF-1.pdf.
- Edi.pleio.nl, 'Wat is een wallet?', te raadplegen via https://edi.pleio.nl/cms/view/c100d3ef-0670-4fee-b47d-bf94eb5b38b4/wat-is-een-wallet.
- EUR-Lex, ‘Veiligere transacties via internet, Samenvatting van: Verordening (EU) nr. 910/2014: betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt’, te raadplegen via https://eur-lex.europa.eu/legal-content/NL/LSU/?uri=CELEX%3A32014R0910.
- Forum Standaardisatie, ‘Handreiking voor overheidsorganisaties: Betrouwbaarheidsniveaus voor digitale dienstverlening’, november 2016, te raadplegen via https://www.forumstandaardisatie.nl/sites/bfs/files/atoms/files/Betrouwbaarheidsniveaus_voor_digitale_dienstverlening_v4.PDF.
- InnoValor (B. Hulsebosch, O. Kulyk & H. de Bos), ‘Biometrie voor identiteitsverificatie: Verkenning van de mogelijkheden’, 20 januari 2020, te raadplegen via https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2020/03/Biometrie-voor-identiteitsverificatie.pdf.
- Integraal Zorg Akkoord, ‘Samen werken aan gezonde zorg’, september 2022, te raadplegen via https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2022/09/16/integraal-zorgakkoord-samen-werken-aan-gezonde-zorg/integraal-zorg-akkoord.pdf.
- KNMG, ‘Alles wat u moet weten over videoconsulten met patiënten’, 27 september 2021, te raadplegen via https://www.knmg.nl/actualiteit-opinie/nieuws/nieuwsbericht/alles-wat-u-moet-weten-over-videoconsulten-met-patienten.
- KNMG-Gedragscode voor artsen, februari 2022, te raadplegen via https://www.knmg.nl/download/knmg-gedragscode-voor-artsen-2.
- KNMG-richtlijn: Omgaan met medische gegevens, november 2022, te raadplegen via https://www.knmg.nl/download/knmg-richtlijn-omgaan-met-medische-gegevens-2.
- KPN, Wat is PiM?’, te raadplegen via https://www.kpn.com/service/pim.htm.

- LHV, ‘Beeldbellen en videoconsult’, te raadplegen via https://www.lhv.nl/thema/patientengegevens-en-ict/beeldbellen-en-videoconsult/.
- Logius, ‘Functionele beschrijving DigiD - Inloggen met app2app’, te raadplegen via https://www.logius.nl/domeinen/toegang/digid/documentatie/functionele-beschrijving-digid-app2app.
- Logius, ‘Handleiding voor aansluiten op DigiD’, onder Keuze Eenmalig inloggen, te raadplegen viahttps://www.logius.nl/domeinen/toegang/digid/documentatie/handleiding-voor-aansluiten-op-digid.
- Logius, ‘Koppelvlakspecificatie DigiD SAML Authenticatie’, onder Herauthenticate en timers, te raadplegen via https://www.logius.nl/domeinen/toegang/digid/documentatie/koppelvlakspecificatie-digid-saml-authenticatie.
- M. Jansen, ‘AVG en beveiliging: passende maatregelen voortaan proactiever nemen en monitoren’, Computerrecht 2017/152.
- M. Sombroek-van Doorm, Medisch beroepsgeheim en de zorgplicht van de arts bij kindermishandeling in de rechtsverhouding tussen arts, kind en ouder, Den Haag: Boom Juridisch 2019, te raadplegen via https://scholarlypublications.universiteitleiden.nl/access/item%3A2979146/view.
- M.C.A. Duijvestijn, ‘Het gebruik van kunstmatige intelligentie bij de beoordeling van kredietwaardigheid van klanten in de bancaire praktijk, Brengt de AI-verordening hier verandering in?’’, MvV 2022, nr. 9, te raadplegen via https://www.bjutijdschriften.nl/tijdschrift/maandbladvermogensrecht/2022/9/MvV_1574-5767_2022_032_009_002.pdf.
- Ministerie van Volksgezondheid, Welzijn en Sport, ‘Is het ook toegestaan om 2-factor authenticatie aan te bieden?’, te raadplegen via https://www.gegevensuitwisselingindezorg.nl/onderwerpen/digitale-toegang/vraag-en-antwoord/is-2f-authenticatie-ook-mogelijk-in-plaats-van-digid-substantieel.
- NOS Nieuws (B. de Vries), ‘Miljoenen snappen digitale overheid onvoldoende, meeste hoofdpijn over DigiD’, 10 juli 2023, te raadplegen via https://nos.nl/artikel/2482218-miljoenen-snappen-digitale-overheid-onvoldoende-meeste-hoofdpijn-over-digid.
- PrivacyCare en PBLQ, ‘Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg’, mei 2016, te raadplegen via https://zoek.officielebekendmakingen.nl/blg-780664.pdf.
- Rijksoverheid, ‘Burgerservicenummer (bsn) in de zorg’, te raadplegen via https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn/bsn-in-de-zorg
- RTL Nieuws (D. Verlaan), ‘Met de nieuwe passkeys mag je jouw wachtwoorden (eindelijk) vergeten’, 28 oktober 2023, te raadplegen via https://www.rtlnieuws.nl/nieuws/nederland/artikel/5415263/passkeys-inloggen-einde-van-wachtwoord.
- Vidua, ‘Onbezorg online identificeren’, te raadplegen via https://vidua.nl/identificeren/.
- VNG, Analyse Samenhang: Europese digitale wetgeving fase 1 Eindrapport, te raadplegen via https://vng.nl/sites/default/files/2023-03/eindrapport-analyse-samenhang-europese-digitale-wetgeving.pdf.
- Yivi, ‘Digital Identity Wallet’, te raadplegen via https://www.yivi.app/en/for-business/yivi-ecosystem.

Rechtspraak

- EHRM 25 februari 1997, ECLI:NL:XX:1997:AD4448, *NJ* 1999/516 m.nt. G. Knigge.

- HvJ EU 6 november 2003, ECLI:EU:2003:596 (*Lindqvist*).
- Regionaal Tuchtcollege voor de Gezondheidszorg Eindhoven 18 november 2022, ECLI:NL:TGZREIN:2022:66, *JGR* 2023/10.
- Conclusie van advocaat-generaal T. Ćapeta 14 september 2023, ECLI:EU:C:2023:676.

Bijlage 1: Juridisch kader vereiste betrouwbaarheidsniveaus inlogmiddelen digitale diensten

1. Inleiding

Onderstaand is het juridisch kader nader uitgewerkt dat geldt voor het bepalen van het vereiste betrouwbaarheidsniveau voor inlogmiddelen voor patiënten als het gaat om digitale dienstverlening door zorgaanbieders. Achtereenvolgens zal worden ingegaan op de wet- en regelgeving die van toepassing is, dit is beperkt tot de voor het onderzochte onderwerp relevante onderdelen van die wet- en regelgeving. Daarbij zijn tevens uitspraken van de Autoriteit Persoonsgegevens als het gaat om het vereiste betrouwbaarheidsniveau voor patiëntauthenticatie, relevante onderzoeken en handreikingen meegenomen. Onderstaand wordt nader ingegaan op:

- (U)AVG): recht op bescherming persoonsgegevens
- Medisch beroepsgeheim
- Wet Digitale Overheid
- de eIDAS-verordening (2.0)

2. Recht op bescherming van persoonsgegevens: (U)AVG

De verwerking van persoonsgegevens is een beperking van het recht op de bescherming van de *persoonlijke levenssfeer* in de zin van artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM), artikel 17 van het Internationaal verdrag inzake burgerlijke en politieke vrijheden, artikel 7 van het EU-Handvest en artikel 10 van de Grondwet.

Daarnaast is het recht op bescherming van *persoonsgegevens* opgenomen in artikel 8 van het EU-Handvest en artikel 16 van het verdrag betreffende de werking van de Europese Unie (VWEU). De verwerking van persoonsgegevens moet voldoen aan de eisen die uit die artikelen voortvloeien. Voor artikel 7 van het EU-Handvest geldt dat het in principe dezelfde reikwijdte en inhoud heeft als artikel 8 van het EVRM. Zoals beschreven in overweging 1 en 12 van de AVG zijn artikel 8 van het EU-Handvest en artikel 16 van het VWEU[60] uitgewerkt in de AVG en overige regelgeving.

U(AVG)

Vanaf 25 mei 2018 is de AVG rechtstreeks van toepassing in alle lidstaten van de Europese Unie en de Europese Economische Ruimte (“EER”). Het doel van de AVG is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de EER.[61] De Uitvoeringswet Algemene Verordening Gegevensbescherming geeft in Nederland uitvoering aan de AVG.

[60] Op basis van artikel 16, tweede lid VWEU.

[61] Artikel 1 AVG.

De AVG vereist dat persoonsgegevens op een rechtmatige, behoorlijke en transparante wijze worden verwerkt.[62] Persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.[63] Zie tevens art. 32 AVG dat de verwerkingsverantwoordelijke en verwerker verplicht de persoonsgegevens die worden verwerkt te beveiligen door passende technische en organisatorische maatregelen te treffen. Hierbij dient rekening te worden gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen.[64] Wat passende maatregelen zijn hangt dus af van de specifieke verwerking en de risico's die daarmee gepaard gaan.[65]

Juistheid en actualiteit

Verder moeten maatregelen worden getroffen waarmee wordt geborgd dat de persoonsgegevens die verwerkt worden juist en actueel zijn. Dit volgt uit artikel 5, eerste lid, aanhef en onder d, van de AVG.

Bijzondere categorieën van persoonsgegevens

Voor de verwerking van de zogeheten bijzondere categorieën van persoonsgegevens gelden specifieke eisen. Het gaat om persoonsgegevens die naar hun aard gevoelig zijn. Het zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over *gezondheid*, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Het verwerken van bijzondere categorieën van persoonsgegevens is verboden, tenzij een van de uitzonderingen genoemd in artikel 9, tweede lid, van de AVG van toepassing is.[66] Deze uitzonderingen zijn op nationaal niveau nader uitgewerkt in paragraaf 3.1 van de UAVG.

---

[62] Artikel 5, eerste lid, sub a AVG.

[63] Artikel 5, eerste lid, sub f, AVG. Ook op grond van artikel 32 AVG moeten verwerkingsverantwoordelijken en verwerkers passende technische en organisatorische maatregelen treffen om een op het risico afgestemde beveiligingsniveau te waarborgen.

[64] Zie ook artikel 25, eerste lid, AVG en overweging 74 van de AVG.

[65] Zie ook B.W. Schermer & J. Toornstra, 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming', 15 april 2023, par. 5.8.

[66] Artikel 9 AVG in samenhang bezien met de artikelen 22 tot en met 30 UAVG.

2.1. Bepalen vereiste betrouwbaarheidsniveau dienstverlening zorgaanbieders aan patiënten

Zoals bovenstaand aangegeven, gaat het bij het bepalen van het vereiste betrouwbaarheidsniveau dus om de vraag welk betrouwbaarheidsniveau kwalificeert als 'passend' in de zin van de AVG. De maatregelen moeten in verhouding staan tot de aard van de gegevens die worden verwerkt en de bijbehorende risico's voor de betrokkenen. Hoe groter het risico voor betrokkenen, des te zwaarder de beveiligingsmaatregelen zijn die getroffen moeten worden. Er is bijvoorbeeld sprake van een hoog risico als op grote schaal bijzondere categorieën van persoonsgegevens worden verwerkt, zoals gezondheidsgegevens. Als het gaat om elektronische dienstverlening van zorgverleners aan patiënten kan hier al snel sprake van zijn. Het uitgangspunt is dat de zorgverlener (als verwerkingsverantwoordelijke) verantwoordelijk is – op basis van een risicoanalyse – voor het bepalen van het betrouwbaarheidsniveau van de verleende diensten.

2.1.1. Criteria voorbeeldcases en jurisprudentie Autoriteit Persoonsgegevens (en voorganger CBP)

De Autoriteit Persoonsgegevens (AP, voorheen CBP) heeft in een aantal voorbeeldcases en jurisprudentie criteria vastgesteld waarmee bepaald kan worden welk betrouwbaarheidsniveau voor digitale dienstverlening van zorgaanbieders van toepassing is.

Hieruit blijkt dat het belangrijkste criterium om vast te stellen welk beveiligingsniveau wordt vereist, of het medisch beroepsgeheim van toepassing is op de persoonsgegevens die worden verwerkt. Met andere woorden; gaat het om 'inlichtingen over de patiënt' zoals bedoeld in art. 7:457 lid 1 BW (WGBO)?

- **2006** Het CBP geeft als antwoord op vragen van het Flevoziekenhuis aan dat 'ook niet-strikt medische zaken onder het begrip "inlichtingen over de patiënt" vallen. De ratio achter het medisch beroepsgeheim is de vertrouwensrelatie tussen patiënt en arts. De arts dient deze vertrouwensrelatie gestalte te geven onder meer door de gegevens die hij in verband met de behandeling van de patiënt verzamelt zo veel mogelijk af te schermen voor anderen. Zoals eerder aangegeven behoren naar het oordeel van het CBP ook afspraakgegevens tot deze categorie.'[67]
- **2013** In het CBP-richtsnoer met betrekking tot beveiliging van persoonsgegevens wordt tevens aangegeven dat het van toepassing zijn van het medisch beroepsgeheim op persoonsgegevens het hoogste beveiligingsniveau vereist: 'bepaalde verwerkingen brengen door de combinatie van de aard van de verwerkte gegevens, de hoeveelheid gegevens die per persoon wordt verwerkt en de doelen waarvoor de persoonsgegevens worden verwerkt dusdanige risico's met zich mee dat het hoogste beveiligingsniveau is vereist. Verwerkingen in deze categorie zijn onder meer verwerkingen bij opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van een grote groep betrokkenen zeer ernstig kunnen worden geschaad indien de verwerkingen onzorgvuldig of onbevoegd geschieden, zoals bij DNA-databanken.

[67] *CBP, Flevoziekenhuis, z2005-1372, 9 mei 2006*

Daarnaast vallen ook verwerkingen waarop een bijzondere geheimhoudingsplicht van toepassing is binnen deze categorie. Deze geheimhoudingsplicht kan door de overheid zowel wettelijk als anderszins formeel zijn geregeld of door een private organisatie zijn ingevoerd voor haar medewerkers[68].

- **In oktober 2016** geeft de AP in een brief aan het bestuur van de NVZ het volgende aan; 'In uitspraken en richtsnoeren heeft de AP regelmatig aangegeven dat bij de patiëntauthenticatie voor communicatie met en onder verantwoordelijkheid van de zorgaanbieder in beginsel dient te worden uitgegaan van een 'hoog betrouwbaarheidsniveau' en dat in gevallen waar het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust het 'hoogste betrouwbaarheidsniveau' vereist is. Het gaat daarmee om een nadere invulling van hetgeen als passend in de zin van artikel 13 Wet bescherming persoonsgegevens (Wbp) wordt aangemerkt.[69]
- **2018** In een brief aan de SG van VWS met betrekking tot patiëntauthenticatie geeft de AP aan dat; 'Gegevens over gezondheid per definitie privacygevoelig zijn. Patiënten moeten erop kunnen vertrouwen dat de informatie die zij met hun arts delen geheim blijft. Daarom gelden voor de bescherming van gegevens over gezondheid extra hoge eisen. Bij haar toezichtstaken moet de AP uitgaan van de geldende wet- en regelgeving op het gebied van de bescherming van persoonsgegevens. In het verleden heeft de AP regelmatig aangegeven dat bij patiëntauthenticatie in het kader van de uitwisseling van gegevens over gezondheid in beginsel dient te worden uitgegaan van een "hoog betrouwbaarheidsniveau" en dat in gevallen waar het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust het "hoogste betrouwbaarheidsniveau" vereist is. In de terminologie van de eIDAS-verordening wil dit zeggen dat bij patiëntauthenticatie minimaal niveau "substantieel" vereist is. Als het gaat om gegevens waarop het medisch beroepsgeheim van de hulpverlener rust, is betrouwbaarheidsniveau "hoog" vereist.[70]

De conclusie is dat als het gaat om een nadere invulling van hetgeen als passend in de zin van artikel 5, eerste lid, sub f, AVG wordt aangemerkt, de AP voor de verwerking van persoonsgegevens waarop het medisch beroepsgeheim rust uitgaat van betrouwbaarheidsniveau hoog.

[68] *CBP richtsnoeren: beveiliging van persoonsgegevens, Stc nr. 5174, 1 maart 2013, p. 15*

[69] *AP, brief bestuur NVZ, twee-factor authenticatie van patiënten bij toegang patiëntenportals, 7 oktober 2016.*

[70] AP, brief aan de SG van VWS, Patiëntauthenticatie, z2018-17577, 4 oktober 2018

2.1.2. Handreiking Betrouwbaarheidsniveaus voor digitale dienstverlening: Forum Standaardisatie

Het Forum Standaardisatie heeft een handreiking voor overheidsorganisaties: Betrouwbaarheidsniveaus voor digitale dienstverlening (de "**Handreiking**") opgesteld.[71]

De Handreiking is bedoeld om een bijdrage te leveren aan een eenduidige bewuste bepaling van het betrouwbaarheidsniveau van elektronische overheidsdiensten. Het bevat daartoe een 'classificatiemodel' dat in feite een vereenvoudigde risicoanalyse is. Het classificatiemodel maakt op basis van verschillende (wettelijke) criteria een generieke koppeling mogelijk tussen (soorten) diensten en betrouwbaarheidsniveaus. Ook geeft de Handreiking indicaties die tot inschaling op een hoger of lager betrouwbaarheidsniveau zouden kunnen leiden. De Handreiking bevat geen vertaling van de betrouwbaarheidsniveaus naar specifieke authenticatiemiddelen. Het classificatiemodel geeft niet onder alle omstandigheden een juiste uitkomst. Er zijn zowel risicoverlagende als risicoverhogende factoren, waarmee door de verantwoordelijke altijd rekening gehouden dient te worden. Zoals uit de titel blijkt is de handreiking gericht op elektronische overheidsdiensten en niet specifiek ontwikkeld voor de elektronische dienstverlening in de zorg. Het is echter zeker ook bruikbaar voor elektronische dienstverlening aan patiënten.

Als er sprake is van bijzondere persoonsgegevens (waaronder gezondheidsgegevens) dient volgens de Handreiking uit te worden gegaan van het betrouwbaarheidsniveau substantieel.

Betrouwbaarheidsniveau: substantieel
Klasse II persoonsgegevens (verhoogd risico)
- Er worden bijzondere persoonsgegevens gebruikt (zoals genoemd in artikel 16 van de Wbp) of financieel-economische gegevens van de betrokkene.

Als het gaat om gegevens die onder het beroepsgeheim vallen (zoals medische gegevens) dient te worden uitgegaan van het betrouwbaarheidsniveau hoog. [72]

Betrouwbaarheidsniveau: hoog
Klasse III persoonsgegevens (hoog risico)
- Er worden gegevens van opsporingsdiensten gebruikt, gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde, geheim-houdingsplicht op rust en gegevens die onder het beroepsgeheim vallen (zoals medische gegevens) in de zin van artikel 9, vierde lid, van de Wbp.

[71] Forum Standaardisatie, 'Handreiking voor overheidsorganisaties: Betrouwbaarheidsniveaus voor digitale dienstverlening', november 2016.

[72] Forum Standaardisatie, 'Handreiking voor overheidsorganisaties: Betrouwbaarheidsniveaus voor digitale dienstverlening', november 2016, p. 33. Artikel 9, vierde lid, van de Wet bescherming persoonsgegevens die inmiddels is vervallen luidde: *"De verwerking van persoonsgegevens blijft achterwege voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat"*.

De volgende versie van de Handreiking wordt begin 2024 verwacht. [73]

2.2. Situatie sinds 2018: gedogen patiëntauthenticatie op betrouwbaarheidsniveau laag

In de brief aan de SG van het Ministerie van VWS in oktober 2018 laat de AP zien dat men zich ervan bewust is 'dat patiëntauthenticatie op betrouwbaarheidsniveaus "substantieel" en "hoog" op dit moment (nog) niet breed beschikbaar is als gebruik wordt gemaakt van DigiD. De AP verwijst naar een brief van de staatssecretaris van BZK aan de Tweede Kamer waarin is toegezegd om in het zogenoemde BSN-domein, waarin doorgaans gebruik wordt gemaakt van DigiD, inlogmethoden met betrouwbaarheidsniveau "substantieel" en "hoog" mogelijk te maken. Daarbij zal allereerst worden gezorgd voor brede beschikbaarheid van inlogmethoden op het niveau "substantieel". De staatssecretaris acht dat van belang omdat de middelen op niveau "hoog" in de komende jaren pas geleidelijk worden ingevoerd, via het natuurlijke vervangingspatroon van de rijbewijzen en de identiteitskaarten.

Tegen deze achtergrond is het uitgangspunt van de AP als volgt*. Zolang een passend betrouwbaarheidsniveau voor patiëntauthenticatie niet kan worden gerealiseerd, mag elektronische uitwisseling van gegevens over gezondheid tussen zorgaanbieders en patiënten in beginsel niet plaatsvinden. De bescherming van persoonsgegevens, waaronder gegevens over gezondheid, is dan onvoldoende gewaarborgd. Zodra binnen het eID-programma inlogmethoden met de betrouwbaarheidsniveaus "substantieel" en "hoog" breed beschikbaar komen, dient een lager betrouwbaarheidsniveau bij de verwerking van gegevens over gezondheid dus niet meer beschikbaar te worden gesteld.*[74]

De AP ziet echter in dat het niet in het belang van de patiënt is dat zorginnovaties stilstaan totdat de passende betrouwbaarheidsniveaus breed beschikbaar zijn binnen het eID-programma. *Daarom is het in eerste instantie van belang dat de nodige voortvarendheid wordt betracht bij de ontwikkeling en het beschikbaar maken van de benodigde betrouwbaarheidsniveaus binnen het eID-stelsel. Verder moet de zorgsector bezien welke mogelijkheden – eventueel buiten DigiD om – momenteel wél beschikbaar zijn om te gebruiken voor patiëntauthenticatie. Zo wordt duidelijk op welke wijze het nieuwe eID-stelsel bij patiënten en zorgaanbieders kan worden geïmplementeerd.*

In afwachting van het breder beschikbaar komen van authenticatiemethoden met een passend hoog niveau, dient authenticatie plaats te vinden met tenminste tweefactorauthenticatie (zoals DigiD in combinatie met sms). Een lagere betrouwbaarheid is in ieder geval niet aanvaardbaar.

[73] Forum Standaardisatie, 'Handreiking voor overheidsorganisaties: Betrouwbaarheidsniveaus voor digitale dienstverlening', november 2016.

[74] Autoriteit Persoonsgegevens, brief aan het Ministerie van Volksgezondheid, Welzijn en Sport, z2018-17577, 4 oktober 2018, par. 4 onder Uitgangspunt van de AP.

Randvoorwaarde daarbij is dat er zo nodig aanvullende maatregelen worden getroffen om openstaande risico's, die niet worden weggenomen met tweefactorauthenticatie, te mitigeren.[75]

Conclusie

De conclusie is dat als het gaat om een nadere invulling van hetgeen als passend in de zin van artikel 5, eerste lid, sub f, AVG wordt aangemerkt, de AP voor de verwerking van persoonsgegevens waarop het medisch beroepsgeheim rust uitgaat van betrouwbaarheidsniveau hoog. Ook in de handreiking zoals opgesteld door het Forum Standaardisatie wordt deze conclusie onderschreven.

Sinds 2018 is sprake van een gedoogsituatie waarbij de zorgaanbieders tenminste gebruik moeten maken van tweefactor authenticatie (eIDAS betrouwbaarheidsniveau laag) zolang inlogmethoden met het betrouwbaarheidsniveau substantieel of hoog niet breed beschikbaar zijn binnen het eID-programma.

Niet duidelijk is echter wanneer sprake is van brede beschikbaarheid en wanneer deze verwacht wordt te zijn bereikt voor bijvoorbeeld betrouwbaarheidsniveau substantieel. Deze onduidelijkheid komt tevens naar voren in het advies van de AP over de consultatieversie van de Regeling betrouwbaarheidsniveaus in oktober 2020. In de toelichting op de regeling wordt door het Ministerie van BZK aangegeven dat "*Het de verwachting is dat twee jaar na inwerkingtreding van deze regeling sprake zal zijn van voldoende beschikbaarheid en dekkingsgraad van (publieke en private) inlogmiddelen.*" De AP betwijfelt of deze termijn van twee jaar nodig en passend is gelet op de huidige stand van de techniek en vooral de snelle technische ontwikkelingen wat betreft inlogmiddelen."[76]

[75] Autoriteit Persoonsgegevens, brief aan het Ministerie van Volksgezondheid, Welzijn en Sport, z2018-17577, 4 oktober 2018, par. 4 onder Wat te doen in de tussentijd.

[76] Autoriteit Persoonsgegevens, brief aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, 15 oktober 2020.

3. Medisch beroepsgeheim en gezondheidsgegevens

Zoals in bovenstaand hoofdstuk beschreven, is voor de vraag welk betrouwbaarheidsniveau bij informatie-uitwisseling tussen zorgaanbieders en patiënten dient te worden toegepast van belang of sprake is van gezondheidsgegevens (tenminste substantieel) óf dat er sprake is van persoonsgegevens waarop het medisch beroepsgeheim van de zorgverlener rust (betrouwbaarheidsniveau hoog). Dit onderscheid leidt in de praktijk tot veel verwarring.

Gezondheidsgegevens: bijzondere persoonsgegevens onder de AVG

Volgens het College Bescherming Persoonsgegevens ("**CBP**") (voorganger van de AP) heeft het begrip gezondheidsgegevens een ruime strekking: "*Het begrip "persoonsgegevens betreffende iemands gezondheid" (art. 16 WBP) heeft een ruime strekking. Volgens de WBP is de loutere mededeling dat iemand ziek is bijvoorbeeld al een gegeven betreffende iemands gezondheid. Ondanks het feit, dat (…) de aanwezigheid van een afspraak op een polikliniek niet altijd tot de gevolgtrekking kan leiden dat iemand ziek is, is er natuurlijk wel degelijk een significante correlatie tussen beide gegevens.*

Daarnaast zijn afspraakgegevens naar hun aard specifieker dan het enkele feit dat iemand ziek is, omdat zij, afhankelijk van de grootte van de afdeling (of polikliniek) en de breedte van de specialisatie een – min of meer nauwkeurig - beeld kunnen geven van de betreffende ziekte."[77]

Onder gezondheidsgegevens (of gegevens over gezondheid) worden de persoonsgegevens verstaan die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.[78] Het begrip gezondheidsgegevens wordt ruim opgevat en omvat gegevens over verleden, heden en toekomst.[79]

Medisch beroepsgeheim

Het medisch beroepsgeheim is verankerd in verschillende wetten (artikel 272 Wetboek van Strafrecht, art. 88 wet BIG, artikel 7:457 BW (WGBO). In de WGBO is vastgelegd dat de

---

[77] CBP, brief aan Flevoziekenhuis, z2005-1372, 9 mei 2006.

[78] Zie artikel 4, onder 15 AVG.

[79] Zie overweging 35 AVG. Zie ook HvJ EU 6 november 2003, ECLI:EU:2003:596, punt 50 (*Lindqvist*): *"(…) een ruime uitleg wordt gegeven, zodat informatie over alle – zowel fysieke als psychische – aspecten van iemands gezondheid daaronder valt."* en Conclusie van advocaat-generaal T. Ćapeta 14 september 2023, ECLI:EU:C:2023:676, punt 97: *"Alle partijen behalve verzoekster merken – terecht – op dat deze definitie uit twee elementen bestaat. Het eerste element is het vereiste dat de betreffende persoonsgegevens verband houden met de lichamelijke of geestelijke gezondheid van een natuurlijke persoon. Het tweede element houdt in dat met die gegevens informatie over de gezondheidstoestand van die persoon wordt verstrekt. Met andere woorden, de persoonsgegevens in kwestie moeten niet alleen op de een of andere manier verband houden met de gezondheid van de betrokkene (wat dus een ruim verband impliceert), maar moeten het ook mogelijk maken om uit die gegevens conclusies te trekken over de gezondheidstoestand van de betrokkene (wat dus een gepersonaliseerd aspect van de betrokken informatie impliceert)."*

hulpverlener, zonder toestemming van de patiënt, geen inlichtingen over de patiënt of inzage in of afschrift van bescheiden mag verstrekken aan derden.[80]

Voorts kan worden gewezen op de vele beroepsregels en gedragsregels die door de beroepsgroep zelf zijn opgesteld,[81] alsmede andere regels en normen die kunnen worden gerekend tot de professionele standaard waaraan een 'goed hulpverlener' is gehouden (art. 7:453 BW). Ook in andere landen en op internationaal niveau heeft het medisch beroepsgeheim erkenning gevonden.[82] Het beschermen van medische gegevens is volgens het Europese Hof voor de Rechten van de Mens ("EHRM") een kernverplichting van de Staat die doorwerkt in de horizontale relatie tussen arts en patiënt.[83]

Veel waarde wordt gehecht aan het medisch beroepsgeheim. Het medisch beroepsgeheim waarborgt de onbelemmerde toegang tot de gezondheidszorg (algemeen belang) en het respect voor de privacy van patiënten (individueel belang). Als patiënten er niet op kunnen rekenen dat alles wat zij met een arts of een andere beroepsbeoefenaar bespreken vertrouwelijk wordt behandeld, komt de toegang tot de zorg in gevaar – en zullen patiënten mogelijk pas later hulp zoeken en een zorgaanbieder wellicht niet alles vertellen. Het stellen van een diagnose en opstellen van een behandelplan worden dan bemoeilijkt, met alle gevolgen van dien voor de individu en de volksgezondheid.[84] Het medisch beroepsgeheim bestaat de facto uit twee componenten: een zwijgplicht en een verschoningsrecht. De op de arts rustende plicht om te zwijgen over alles dat hij in het kader van de beroepsuitoefening over de patiënt te weten is gekomen, vloeit voort uit het recht van de patiënt op vertrouwelijke omgang met persoonlijke (gezondheids)gegevens. Op grond van het verschoningsrecht mogen artsen zich voor de rechter verschonen van het afleggen van een getuigenis en het beantwoorden van vragen als zij, door te spreken, in strijd zouden komen met hun beroepsgeheim.[85]

Over de ratio van het medisch beroepsgeheim stelt het CBP het volgende:

"*De ratio achter het medisch beroepsgeheim is de vertrouwensrelatie tussen patiënt en arts. De arts dient deze vertrouwensrelatie gestalte te geven onder meer door de gegevens die hij in verband met de behandeling van de patiënt verzamelt zo veel mogelijk af te schermen voor*

[80] Zie artikel 7:457, eerste lid, BW.

[81] Zie bijv. nr. 5 van de KNMG-Gedragscode voor artsen, februari 2022: *"Als arts bewaak en bevorder je de vertrouwensrelatie met de patiënt. Je houdt geheim wat je tijdens je beroepsuitoefening te weten komt over de patiënt".*

[82] A. Hendriks, 'Het medisch beroepsgeheim. Enige actuele dilemma's', *NJCM-Bulletin* 2001, jrg. 26, nr. 5, p. 525-538.

[83] EHRM 25 februari 1997, ECLI:NL:XX:1997:AD4448, *NJ* 1999/516 m.nt. G. Knigge. Zie ook M. Sombroek-van Doorm, *Medisch beroepsgeheim en de zorgplicht van de arts bij kindermishandeling in de rechtsverhouding tussen arts, kind en ouder*, Den Haag: Boom Juridisch 2019, p. 1.

[84] A.C. Hendriks, Het medisch beroepsgeheim anno 2016: gewenste en ongewenste veranderingen, *Tijdschrift voor Gezondheidsschade, Milieuschade en Aansprakelijkheidsrecht* 2015, afl. 4, p. 164.

[85] A. Hendriks, 'Het medisch beroepsgeheim. Enige actuele dilemma's', *NJCM-Bulletin* 2001, jrg. 26, nr. 5, p. 527-528.

anderen. Zoals eerder aangegeven behoren naar het oordeel van het CBP ook afspraakgegevens tot deze categorie." [86]

Van belang voor het voorliggende vraagstuk is wat nu verstaan moet worden onder 'inlichtingen over de patiënt, inzage in bescheiden of afschrift van bescheiden'? In het gezondheidsrecht is een brede interpretatie van de reikwijdte van het medisch beroepsgeheim aangewezen.[87]

Het (medisch) beroepsgeheim omvat alle informatie die een arts in de uitoefening van zijn beroep over een patiënt te weten komt. Ook het enkele feit dat een patiënt onder behandeling is bij een arts, valt al onder het beroepsgeheim. Daarnaast geldt het beroepsgeheim onder meer voor:
* informatie die een patiënt zelf aan een arts toevertrouwt;
* gegevens die de arts over de patiënt verzamelt, zoals de anamnese, diagnose, laboratoriumuitslagen, röntgenfoto's, behandeling en medicatie;
* informatie die de arts buiten de patiënt te weten komt;
* informatie die anderen over de patiënt verstrekken; en
* niet medische informatie, zoals NAW-gegevens, informatie over de gezinssituatie of privéomstandigheden van de patiënt.[88]

Het beroepsgeheim omvat daarmee alle gegevens, die een arts in de uitoefening van zijn beroep over de patiënt te weten komt, ook niet medische zaken en zaken die de arts buiten de patiënt om te weten komt.

Voorbeeld: politie vraagt een arts of deze een bepaalde persoon heeft behandeld of in de praktijk heeft gezien, arts geeft geen antwoord. [89] De informatie of iemand onder behandeling is bij een zorgaanbieder valt dus onder het medisch beroepsgeheim. Uit bijlage 1 van de basisprincipes medisch beroepsgeheim van de Rijksoverheid: '*Alles wat de hulpverlener in de uitoefening van zijn beroep over de patiënt te weten is gekomen valt onder het medisch beroepsgeheim. Dat kunnen ook niet medische zaken zijn zoals de gezinssituatie of privéomstandigheden. Het enkele feit dat de patiënt een afspraak heeft met een hulpverlener valt ook onder het geheim."*[90]

---

[86] CBP, brief aan Flevoziekenhuis, z2005-1372, 9 mei 2006.

[87] H.J.J. Leenen e.a. Handboek gezondheidsrecht, Boom Juridisch: Den Haag, p. 141. Zie ook M. Sombroek-van Doorm, *Medisch beroepsgeheim en de zorgplicht van de arts bij kindermishandeling in de rechtsverhouding tussen arts, kind en ouder*, Den Haag: Boom Juridisch 2019, p. 108.

[88] KNMG-richtlijn: Omgaan met medische gegevens, november 2022, p. 15. Zie ook Regionaal Tuchtcollege voor de Gezondheidszorg Eindhoven 18 november 2022, ECLI:NL:TGZREIN:2022:66, r.o. 4.17, *JGR* 2023/10: "*Het beroepsgeheim omvat alle informatie die een arts in de uitoefening van zijn beroep over een patiënt te weten komt. Ook het enkele feit dat een patiënt onder behandeling is bij een (andere) arts, valt onder het beroepsgeheim.*"

[89] Handreiking KNMG, Beroepsgeheim en politie/justitie, p. 11. Zie ook Regionaal Tuchtcollege voor de Gezondheidszorg Eindhoven 18 november 2022, ECLI:NL:TGZREIN:2022:66, r.o. 4.17, *JGR* 2023/10*: "Het beroepsgeheim omvat alle informatie die een arts in de uitoefening van zijn beroep over een patiënt te weten komt. Ook het enkele feit dat een patiënt onder behandeling is bij een (andere) arts, valt onder het beroepsgeheim."*

[90] https://www.rijksoverheid.nl/documenten/rapporten/2016/06/15/basisprincipes-medisch-beroepsgeheim

Conclusie

In de praktijk is er verwarring als het gaat om het onderscheid tussen gezondheidsgegevens en persoonsgegevens waarop het medisch beroepsgeheim van toepassing is. Als het gaat om de vraag of het betrouwbaarheidsniveau hoog van toepassing is dan gaat de discussie vaak over of er nu wel of niet sprake is van een gezondheidsgegeven en wat dit dan zegt over de gezondheid van de patiënt. Het criterium of wel of niet sprake is van gezondheidsgegevens in de communicatie tussen zorgaanbieder en patiënt is niet het doorslaggevende criterium voor het bepalen van het passende niveau. Dit wordt bepaald door het wel of niet van toepassing zijn van het medisch beroepsgeheim op de betreffende gegevens. Zoals eerder aangegeven, is het medisch beroepsgeheim tenslotte ook van toepassing op niet medische zaken. Een afspraak met een zorgverlener valt ook onder dit geheim.

4. Wet digitale overheid; kaderwet

De Wet digitale overheid (Wdo) regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. Daarmee wordt bedoeld dat burgers elektronische identificatiemiddelen ("eID") krijgen met een substantiële of hoge mate van betrouwbaarheid. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit. [91] Het wetsvoorstel van de Wdo maakt het mogelijk om straks via publieke én private inlogmiddelen digitaal zaken te doen met bijvoorbeeld gemeenten en zorgaanbieders (voor zover deze onder de reikwijdte van de Wdo vallen). Alleen middelen die door de overheid op veiligheid en betrouwbaarheid zijn gecontroleerd worden toegelaten.[92] Die zijn dan in het publieke domein toegestaan. Hoewel inloggen bij diensten van commerciële/private partijen zoals webwinkels niet in de Wdo wordt geregeld, wordt aangegeven dat het de bedoeling is dat burgers met de gecontroleerde private middelen ook daar kunnen inloggen.[93]

Na (volledige) inwerkingtreding geldt voor de organisaties die onder de reikwijdte van de Wdo vallen onder andere dat:

- zij hun digitale diensten moeten indelen naar betrouwbaarheidsniveaus;
- zij een acceptatieplicht hebben voor toegelaten inlogmiddelen;
- zij hun informatiebeveiliging op orde moeten hebben.

De Wdo sluit aan bij Europese ontwikkelingen in digitale overheidsdienstverlening en inloggen bij de overheid. De toe te laten publieke en private inlogmiddelen moeten voldoen aan de Europese eisen (i.c. eIDAS-verordening).

De Minister van BZK is verantwoordelijk voor de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de generieke digitale infrastructuur[94] (stelsel Toegang). De techniek (ICT) en de organisatie achter het stelsel Toegang zijn momenteel in ontwikkeling. Zodra dit gereed is, is het stelsel toegankelijk voor dienstverleners en kunnen inlogmiddelen erkend worden. Binnen het stelsel zal onder andere worden voorzien in erkende inlogmiddelen die voldoen aan de eisen, een routeringsvoorziening en een machtigingsvoorziening.
De routeringsvoorziening helpt om het stelsel te ontsluiten, dienstverleners kunnen er ook voor kiezen om gebruik te maken van een private ICT-dienstverlener om aan te sluiten of het zelf regelen. Vervolgens kunnen dienstverleners alle toegelaten middelen accepteren en daarmee voldoen aan de acceptatieplicht. Burgers en bedrijven kunnen zo van alle toegelaten middelen gebruik maken om langs digitale weg diensten af te nemen.

[91] Digitale Overheid, 'Wet digitale overheid'.

[92] Zie ook Digitale Overheid, 'Toelating en aansluiting van publieke & private middelen en diensten.

[93] Digitale overheid, 'Wet digitale overheid'.

[94] Artikel 5 Wdo.

De Wdo ziet op de digitale overheid. Er is voor gekozen om de Wdo ook van toepassing te laten zijn op zorgaanbieders. Zorgaanbieders zijn aangewezen organisaties zoals bedoeld in artikel 2, tweede lid, sub a Wdo). In de bijlage bij artikel 2, tweede lid, onder a, Wdo is opgenomen dat de Wdo ook van toepassing is op zorgaanbieders, categorieën van indicatieorganen en categorieën van zorgverzekeraars die vallen onder de Wabvpz, in het kader van de taken waarvoor zij op basis van de Wdo het burgerservicenummer gebruiken.[95]

De Wdo is een kaderwet, uitwerking vindt plaats in de lagere regelgeving. Zoals in algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen. Hiervoor is gekozen om ruimte te laten voor innovatie, verdere keuzes en nieuwe voorzieningen en functionaliteiten.

4.1. Eerste tranche Wdo: gefaseerde invoering

De eerste tranche (deel) van de Wdo, is op 1 juli 2023 in werking getreden. Onderstaand worden de voor het vraagstuk van dit rapport meest relevante onderdelen beschreven. In paragraaf 4.2 zal nader worden ingegaan op de relevante artikelen en lagere wet- en regelgeving die nog niet in werking zijn getreden.

Betrouwbaarheidsniveaus: artikel 6 Wdo, Regeling Betrouwbaarheidsniveaus
Artikel 6 Wdo ziet op de betrouwbaarheidsniveaus als het gaat om toegang tot elektronische dienstverlening. De Wdo volgt de betrouwbaarheidsniveaus van de eIDAS-verordening: laag, substantieel en hoog. In het eerste lid is geregeld dat bij elektronische dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, bestuursorganen en aangewezen organisaties uitsluitend toegang tot de dienstverlening verlenen indien gebruik wordt gemaakt van identificatiemiddelen die ten minste het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau hebben.

Dit artikel is vanaf 1 juli 2023 in werking, voor de zorgaanbieder betekent dit als het gaat om het vereiste betrouwbaarheidsniveau niet echt iets nieuws. Zoals eerder beschreven is de zorgaanbieder nu ook al verantwoordelijk om te zorgen voor een passend beveiligingsniveau. De Wdo concretiseert deze verplichting.

In artikel 6, tweede lid, Wdo is opgenomen dat bestuursorganen en aangewezen organisaties volgens bij ministeriële regeling te stellen regels bepalen voor welke door hen te verlenen elektronische diensten authenticatie op een bepaald betrouwbaarheidsniveau vereist is. Dit is nader uitgewerkt in de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening (Regeling betrouwbaarheidsniveaus).

Regeling betrouwbaarheidsniveaus
(Semi-) overheidsdiensten moeten de diensten die zij verlenen en waarbij elektronische toegang mogelijk is indelen in betrouwbaarheidsniveau laag, substantieel of hoog. In de Regeling

betrouwbaarheidsniveaus worden nadere regels gesteld over de criteria die door publieke dienstverleners moeten worden gehanteerd.[96] Deze regeling is 1 juli 2023 in werking getreden.

Op grond van artikel 2, tweede lid, Regeling betrouwbaarheidsniveaus juncto bijlage 2 bij de Regeling betrouwbaarheidsniveaus wordt geconcludeerd dat (in het geval niet bij wettelijk voorschrift is bepaald dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is) betrouwbaarheidsniveau hoog vereist is als het gaat om gegevens die onder het medisch beroepsgeheim vallen.

Op grond van artikel 2, derde lid, Regeling betrouwbaarheidsniveaus juncto bijlage 2 bij de Regeling betrouwbaarheidsniveaus wordt geconcludeerd dat (in het geval niet bij wettelijk voorschrift is bepaald dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is) betrouwbaarheidsniveau substantieel vereist is als het om bijzondere categorieën van persoonsgegevens (zoals gegevens over gezondheid)[97] gaat.

In bijlage 2 bij de Regeling betrouwbaarheidsniveaus is daarnaast opgenomen als criterium voor betrouwbaarheidsniveau hoog dat het BSN wordt verwerkt in combinatie met andere persoonsgegevens.

Vaststellen betrouwbaarheidsniveau dienst één niveau lager

Risicoverlagende factoren

In artikel 3, eerste lid Regeling betrouwbaarheidsniveaus is geregeld dat een bestuursorgaan of aangewezen organisatie voor een elektronische dienst authenticatie op één betrouwbaarheidsniveau lager kan vaststellen, indien:
a. het proces van toegangsverlening voorziet in een adequate aanvullende technische of fysieke controle op de authenticiteit van de gebruiker van het identificatiemiddel na het moment waarop daarmee voor de eerste keer voor de desbetreffende dienst een authenticatie is uitgevoerd;
b. het bestuursorgaan of de aangewezen organisatie in het proces herstelmaatregelen neemt of kan nemen.
Als artikel 3, eerste lid, Regeling betrouwbaarheidsniveaus wordt toegepast sluit dit gelijktijdige toepassing van artikel 6 Regeling betrouwbaarheidsniveaus uit.[98]

Risicoverhogende factoren

In artikel 4 Regeling betrouwbaarheidsniveaus is geregeld dat indien naar het oordeel van het bestuursorgaan of de aangewezen organisatie, gelet op de aard van de dienst, sprake is van risicoverhogende factoren waaronder identiteitsfraude of misbruik van de dienst, wordt een volledige risicoanalyse uitgevoerd teneinde het passende betrouwbaarheidsniveau voor die dienst te kunnen bepalen.

---

[96] Toelichting bij het Conceptbesluit identificatiemiddelen, par. 2.2.

[97] Artikel 1 Regeling betrouwbaarheidsniveaus juncto artikel 1 van de Uitvoeringswet Algemene verordening gegevensbescherming en artikel 9, eerste lid, AVG.

[98] Zie ook artikel 6, tweede lid, Regeling betrouwbaarheidsniveaus.

Tijdelijk één betrouwbaarheidsniveau lager

Artikel 6, vierde lid Wdo biedt de mogelijkheid om bij ministeriële regeling regels te stellen over het gedurende een bepaalde periode toestaan van toegang tot diensten, waarvoor volgens de krachtens het tweede lid gestelde regels authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, met gebruikmaking van door Onze Minister aangewezen identificatiemiddelen die het betrouwbaarheidsniveau laag respectievelijk substantieel hebben.

Dit is nader uitgewerkt in artikel 6, eerste lid Regeling betrouwbaarheidsniveaus. Hierin is opgenomen dat onverminderd de toepasselijkheid van een wettelijk voorschrift dat bepaalt dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is, een bestuursorgaan of aangewezen organisatie, indiende beschikbaarheid of het gebruik van identificatiemiddelen op de betrouwbaarheidsniveaus substantieel en hoog of de mogelijkheid om deze te gebruiken om toegang te krijgen tot dienstverlening onvoldoende is, voor een elektronische dienst, waarvoor authenticatie op betrouwbaarheidsniveau hoog respectievelijk substantieel benodigd is, tot twee jaar na inwerkingtreding van deze regeling voor toegang tot die dienst tevens het gebruik van een toegelaten of erkend middel op betrouwbaarheidsniveau substantieel respectievelijk een middel op betrouwbaarheidsniveau laag toestaan. Gelijktijdige toepassing met artikel 3 Regeling betrouwbaarheidsniveaus wordt uitgesloten. [99]

Voor dit artikel lijkt het uitgangspunt te zijn geweest dat het stelsel Toegang gereed zou zijn bij de inwerkingtreding van de regeling en dat er toegelaten of erkende middelen beschikbaar zouden zijn (koppeling lager niveau aan toegelaten en erkende middelen). Dat is nog niet het geval. Onduidelijk is daarmee hoe dit artikel in de praktijk moet worden geïnterpreteerd. Wellicht zal de overgangsperiode van twee jaar worden verlengd nadat toegelaten of erkende middelen beschikbaar zijn.

4.2. Artikelen Wdo nog niet in werking: acceptatieplicht, toegelaten middelen

Voor de inwerkingtreding van een aantal artikelen van de Wdo is van belang dat de ontwikkeling van de techniek (ICT) en de organisatie achter het stelsel Toegang afgerond is. Uit gesprekken komt naar voren dat nog niet duidelijk is wanneer het stelsel gereed is. Er wordt voorzien dat het meer tijd zal kosten dan in de oorspronkelijke planning opgenomen. De planning die nu nog wordt gecommuniceerd is: de techniek (ICT) en de organisatie achter het stelsel Toegang zijn naar verwachting in 2024 klaar. Dat betekent dat het stelsel toegankelijk voor dienstverleners zou moeten zijn en dat inlogmiddelen erkend kunnen worden. Het is de bedoeling dat alle dienstverleners in de komende 3 jaar zich aansluiten op het stelsel. Ook is het de bedoeling dat alle overheidsorganisaties in de tweede helft van 2026 op het nieuwe stelsel over zijn.[100]

[99] Artikel 6, tweede lid, Regeling betrouwbaarheidsniveaus. Zie ook artikel 3, tweede lid, Regeling betrouwbaarheidsniveaus.

[100] Digitale Overheid, 'Veelgestelde vragen over de inwerkingtreding van de Wdo'.

De voor dit rapport relevante artikelen van de Wdo die nog niet in werking zijn, regelen onder andere het volgende:
- een acceptatieplicht voor toegelaten identificatiemiddel en digitale machtigingsverklaringen[101]
- zorgaanbieders moeten de informatiebeveiliging op orde hebben.[102]

Artikel 7 Wdo, acceptatieplicht (nog niet in werking)
In artikel 7, tweede lid Wdo is opgenomen dat; aangewezen organisaties accepteren bij hun elektronische dienstverlening aan natuurlijke personen waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is uitsluitend:
a. alle toegelaten identificatiemiddelen,
b. elektronische verklaringen als bedoeld in artikel 5, eerste lid, onderdeel b, en
c. onverminderd het bepaalde in artikel 6 van de eIDAS-verordening, alle identificatiemiddelen die behoren tot een door een lidstaat van de Europese Unie ingevolge de eIDAS-verordening bij de Europese Commissie aangemeld en goedgekeurd stelsel indien dit is bepaald bij besluit van Onze Minister in overeenstemming met Onze Minister die het mede aangaat.

Dit betekent voor zorgaanbieders dat nadat de acceptatieplicht van kracht is uitsluitend toegelaten en erkende identificatiemiddelen gebruikt mogen worden, niet toegelaten en erkende middelen mogen daarmee dus niet meer worden geaccepteerd.

Inwerkingtreding acceptatieplicht art. 7 Wdo
In artikel 29, derde lid, Wdo wordt bepaald dat de in de artikel 7 Wdo opgenomen acceptatieplicht voor een aangewezen organisatie niet eerder van toepassing is dan nadat die aangewezen organisatie kan worden aangesloten op de in artikel 5, eerste lid, onderdelen a tot en met e, en tweede lid Wdo bedoelde infrastructuur en voorzieningen overeenkomstig het bij regeling van Onze Minister, gehoord Onze Ministers die het mede aangaat, op te stellen aansluitschema. Het aansluitschema kan erin voorzien dat de acceptatieplichten voor verschillende diensten van een bestuursorgaan of aangewezen organisatie op verschillende momenten van toepassing worden.

Voor de zorgaanbieder betekent dit dat ook nadat de acceptatieplicht in artikel 7 Wdo in werking treedt, deze niet eerder van toepassing is dan nadat de zorgaanbieder ook daadwerkelijk kan worden aangesloten op het stelsel Toegang. Dit zal dan plaatsvinden op basis van een aansluitschema. De Wdo gaat dus pas volledig gelden als een instantie technisch en organisatorisch klaar is om aan te sluiten. De departementen, de publieke dienstverleners en Logius stellen samen een aansluitschema op. Dit aansluitschema gaat een planning bevatten met data waarop de specifieke onderdelen van de wet voor welke instantie van kracht worden. [103]

[101] Zie artikel 7 Wdo. Dit artikel is nog niet in werking getreden. Een toegelaten identificatiemiddel wordt in de Wdo omschreven als een identificatiemiddel voor een natuurlijke persoon dat is aangewezen ingevolge artikel 9 Wdo.

[102] Zie artikel 4 Wdo.

[103] Digitale overheid, 'Wet digitale overheid'.

Afwijking acceptatieplicht art. 7 Wdo
In artikel 7, vierde lid Wdo is een mogelijkheid opgenomen om af te wijken van de acceptatieplicht indien dit noodzakelijk is gelet op de aard van de dienstverlening of de aard van de doelgroep. Een bestuursorgaan, aangewezen organisatie of rechterlijke instantie kan volgens bij ministeriële regeling te stellen regels voor een welbepaalde doelgroep afwijken van het gestelde in het eerste lid, onderdeel a, respectievelijk het tweede lid onderdeel a, indien acceptatie van niet-toegelaten identificatiemiddelen onder uitsluiting van toegelaten identificatiemiddelen noodzakelijk is gelet op de aard van de dienstverlening of de aard van de doelgroep.

Artikel 9 Wdo, toelaten identificatiemiddelen en diensten (nog niet in werking)
De toelatingseisen worden opgenomen in lagere regelgeving. In het Besluit identificatiemiddelen zal worden uitgewerkt op welke wijze de Minister BZK beoordeelt of authenticatiemiddel en een daarbij behorende authenticatiedienst kan worden toegelaten. Met dit besluit zal uitvoering worden gegeven aan artikel 9 Wdo. Dat artikel (dat nog niet in werking is getreden) regelt dat identificatiemiddelen voor burgers door de Minister BZK kunnen worden toegelaten door middel van een erkenning of aanwijzing als deze voldoen aan nader te stellen eisen. Zowel de eisen voor toetsing als de eisen waaraan een toegelaten middel moet voldoen zal met het Besluit identificatiemiddelen worden vastgelegd. Dit besluit zal de toelating, en daarmee ook de acceptatie, van identificatiemiddelen in een nationale context regelen. Dit wordt nader uitgewerkt in Regeling nadere eisen toelating identificatiemiddelen Wdo[104] Aan deze middelen worden eisen gesteld om de veiligheid en privacy te borgen. Daarop wordt gecontroleerd voordat middelen worden toegelaten en vervolgens wordt er toezicht op gehouden. De regeling vult deze eisen meer specifiek in, zoals de eisen rond open source, het verhandelverbod en privacy by design.

In dit kader is het volgende nog relevant. In artikel 2.13 van de conceptregeling nadere eisen toelating identificatiemiddelen Wdo is een verbod opgenomen voor een identificatiemiddel waarbij authenticatie plaatsvindt met gebruik van biometrische gegevens: *"Het authenticatiemechanisme van een identificatiemiddel op betrouwbaarheidsniveau substantieel en hoog maakt geen gebruik van een inherente authenticatiefactor, als bedoeld in de bijlage bij Uitvoeringsverordening (EU) 2015/1502."*

Hierover is in de toelichting – voor zover relevant – het volgende opgenomen: *"Het gebruik van biometrische kenmerken voor authenticatie is in de afgelopen jaren sterk toegenomen. In deze regeling is bepaald dat een erkenning niet wordt verleend voor een identificatiemiddel waarbij authenticatie plaatsvindt met gebruik van biometrische gegevens. De beschikbare techniek en de vele varianten die daarvoor in omloop zijn hebben nog niet een niveau bereikt dat voldoende is voor verantwoorde toepassing bij toegang tot elektronische overheidsdiensten. Wanneer de kwaliteit van deze techniek verbetert of wanneer internationale ontwikkelingen daartoe aanleiding geven kan deze regeling worden gewijzigd om authenticatie met gebruik van biometrische*

[104] https://www.internetconsultatie.nl/regtoelidentmidd/document/9540. *In twee algemene maatregelen van bestuur zijn de kernbepalingen opgenomen ten aanzien van bescherming van gegevens, betrouwbaarheid van authenticaties en de besluitvormingsprocedure. Voor het overige bevatten deze algemene maatregelen van bestuur een basis om nadere eisen en regels te stellen bij ministeriële regeling. De onderhavige ministeriële regeling is daarop gebaseerd en bevat de aanvullende, meer gedetailleerde eisen waaraan wordt getoetst, aanvullende regels over de aanvraagprocedure voor een erkenning en nadere verplichtingen voor houders van een erkenning of aanwijzing."*

gegevens alsnog mogelijk te maken. Deze regeling staat in beginsel niet in de weg aan verificatie van de identiteit (dus vaststelling van de identiteit ten tijde van uitgifte van een identificatiemiddel) met gebruik van biometrie. Voor die toepassing zal in een aanvang moeten worden onderbouwd dat de gebruikte techniek voldoende betrouwbaar is om op het gewenste betrouwbaarheidsniveau te worden gebruikt."

Ook voor het Besluit identificatiemiddelen en de bijbehorende regeling geldt dat deze pas in werking kunnen treden als het stelsel Toegang gereed is.

Voorstel Besluit digitale overheid, artikel 4 en 16 Wdo

Op dit moment is een wetsvoorstel Besluit digitale overheid ("Bdo") in procedure. Het Bdo zal de onderwerpen persoonsgegevensverwerking en informatieveiligheid in het kader van de toegang tot elektronische overheidsdienstverlening reguleren. In het bijzonder zal het Bdo ter uitvoering van de artikelen 4 en 16 van de Wdo dienen.[105]

Besluit directe bevraging gezagsmodule

Met dit conceptbesluit directe bevraging gezagsmodule wordt mogelijk gemaakt dat overheidsinstanties kunnen opvragen welke personen gezag hebben over een minderjarige. Dit besluit wijzigt het Besluit digitale overheid in verband met regels over directe bevraging van de gezagsmodule.

5. eIDAS-verordening

De eIDAS-verordening van het Europees Parlement en de Raad van 23 juli 2014 is per 1 juli 2016 van kracht geworden. Deze verordening gaat over de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en leidt tot een wettelijk kader voor betrouwbaarheidsniveaus. De eIDAS-verordening regelt daartoe het grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de Europese Unie.

De eIDAS-verordening kent drie betrouwbaarheidsniveaus: laag, substantieel en hoog.[106] Deze zijn nader uitgewerkt in een uitvoeringsverordening[107]. De betrouwbaarheidsniveaus, zoals in de eIDAS- verordening zijn opgenomen, worden ook in de AVG en Wdo toegepast.

[105]Artikel 4 Wdo is nog niet in werking getreden en artikel 16 Wdo is deels in werking getreden.

[106] Zie artikel 6 eIDAS-verordening.

[107] Uitvoeringsverordening van de Commissie van 8 september tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

Een elektronische identificatie die in een EU-land wordt toegekend, moet in alle andere EU-landen worden erkend. Dit is slechts van toepassing wanneer de elektronische identificatie aan de eisen van de eIDAS-verordening voldoet, is aangemeld bij de Commissie en is opgenomen in een lijst.[108]

Een stelsel voor elektronische identificatie moet een van de drie betrouwbaarheidsniveaus vermelden (laag, substantieel en hoog) op grond van dat stelsel uitgegeven vormen van elektronische identificatie. Wederzijdse erkenning is alleen verplicht wanneer de relevante overheidsinstantie de betrouwbaarheidsniveaus substantieel" of „hoog" gebruikt om toegang te krijgen tot de online diensten.[109] Nederlandse overheidsorganisaties en private organisaties met een publieke taak moeten sinds 29 september 2018 Europees erkende inlogmiddelen accepteren in hun digitale dienstverlening. Concreet betekent dit dat burgers die de beschikking hebben over een erkend inlogmiddel dezelfde zaken moeten kunnen regelen als alle andere burgers in een EU-lidstaat.[110]

Momenteel geldt deze acceptatieplicht alleen voor academische ziekenhuizen en zorgverzekeraars.

Voorstel herziening eIDAs-verordening; eIDAS 2.0
Op 3 juni 2021 kwam de Europese Commissie met een voorstel voor herziening van de eIDAS-verordening uit 2014.[111] Daarin staat dat elke lidstaat een elektronische identiteit (eID) en minstens één digitale portemonnee (wallet) moet ontwikkelen die in heel Europa geldt. De Europese Commissie wil een digitale portemonnee voor alle burgers, ingezetenen en bedrijven in de Europese Unie. In deze 'European Digital Identity Wallet' kan de nationale digitale identiteit worden gekoppeld aan persoonlijke 'attributen', zoals rijbewijs, diploma's en bankrekening. Het voorstel is nog niet van kracht: eerst moeten alle lidstaten hun standpunt bepalen, daarna wordt in de Raad van de EU onderhandeld over de exacte invulling.

Aanleiding voor dit herzieningsvoorstel is dat in de markt een nieuwe omgeving ontstaat waarin de aandacht verschuift van de levering en het gebruik van rigide digitale identiteiten naar de levering van en een vertrouwen op specifieke attributen die met die identiteiten verbonden zijn. Er is een groeiende vraag naar elektronische identiteitsoplossingen die deze functionaliteiten kunnen bieden, waarmee efficiëntiewinst en een hoog niveau van vertrouwen in de EU, in de particuliere alsook in de publieke sector, worden bewerkstelligd, vanuit de behoefte om gebruikers met een hoge mate van zekerheid te kunnen identificeren en authenticeren.

[108] Zie ook 'EUR-Lex, 'Veiligere transacties via internet, Samenvatting van: Verordening (EU) nr. 910/2014: betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt'.

[109] Zie artikel 8 eIDAS-verordening. Zie ook EUR-Lex, 'Veiligere transacties via internet, Samenvatting van: Verordening (EU) nr. 910/2014: betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt'.

[110] Digitale Overheid, 'eIDAS – Digitale Overheid'.

[111] Voorstel voor een Verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit.

Uit de evaluatie van de eIDAS-verordening is gebleken dat de huidige verordening niet aan deze nieuwe marktbehoefte kan voldoen, vooral vanwege de inherente beperking ervan tot de overheidssector, de beperkte mogelijkheden en de complexiteit voor particuliere aanbieders van onlinediensten om zich op het systeem aan te sluiten, de ontoereikende beschikbaarheid van aangemelde eID-oplossingen in alle lidstaten en het gebrek aan flexibiliteit om uiteenlopende use cases te ondersteunen.[112]

Om te zorgen dat alle burgers en bedrijven, volgens de doelstelling van de herziene eIDAS-verordening, in 2025 gebruik kunnen maken van een hoogwaardige wallet heeft de Minister van BZK een programma ingericht dat een eerste versie van een Nederlandse open source wallet zal neerzetten. De planning is om de eerste versie van deze wallet in 2023 werkend te hebben.[113]

[112] VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit.

[113] Brief van BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal, 17 augustus 2022.

Bijlage 2: Overzicht artikelen en leden van de Wdo die nog niet in werking zijn getreden

Artikel	Omschrijving	Opmerking
1.	Definities	
2.	Reikwijdte	
3.	Standaarden	
4.	Informatieveiligheid	Nog niet in werking getreden.
5.	Verantwoordelijkheid voor het beheer	Lid 1, onder g is nog niet in werking getreden. Ook lid 6 is nog niet in werking getreden.
6.	Betrouwbaarheidsniveaus	
7.	Acceptatie	Nog niet in werking getreden.
8.	Gebruik in publieke domein	
9.	Toelaten van identificatiemiddelen en diensten	Nog niet in werking getreden.
10.	Regels ten aanzien van gebruik	
11.	Erkenning bedrijfs- en organisatiemiddel en bijbehorende diensten	Nog niet in werking getreden.
12.	Aanwijzing van attributen	Nog niet in werking getreden.
13.	Rechten en plichten voor erkende diensten	Nog niet in werking getreden.
14.	Intrekking en overdracht van erkenning	Nog niet in werking getreden.

15.	Acceptatie bedrijfs- en organisatiemiddelen	Nog niet in werking getreden.
16.	Bescherming persoonsgegevens	Leden 2 en 3 zijn nog niet in werking getreden.
17.	Toezicht en handhaving	Leden 3, 5 en 7 zijn nog niet in werking getreden.
18.	Bijzondere bevoegdheden	
19.	Informatieverstrekking	
20.	Leges voor verstrekking publiek identificatiemiddel	
21.	Doorberekening kosten	Nog niet in werking getreden.
22.	Doorberekening aanvraag erkenning en toezicht op naleving erkenningseisen	Nog niet in werking getreden.
23.	Evaluatie	
24.	Overgangsrecht bedrijfs- en organisatiemiddel	Nog niet in werking getreden.
25.	Parlementair betrokkenheid bij gedelegeerde regelgeving	
26.	Innovatie	
27.	Wijziging Wegenverkeerswet 1994	Nog niet in werking getreden.
28.	Omhangen	
29.	Inwerkingtreding	
30.	Citeertitel	

Bijlage 3: Lijst geïnterviewde partijen

We hebben tijdens ons onderzoek de volgende partijen geïnterviewd of we hebben informatie van hen ontvangen.

- Actiz (Annemiek Mulder en Jolanda Dircks)
- BeterDichtbij (Godfried Bogaerts)
- Chipsoft (Olav Trauschke, Vincent van den Berg en Jeffrey Harders)
- Cleverbase/Vidua (Sander Dijkhuis en Remco van Wijk)
- Cor Franke
- De Nederlandse GGZ (Jaap Schrieke)
- Digidentity (Marcel Wendt)
- Dutch Health Leaders Foundation (Douwe Jippes)
- Federatie Medisch Specialisten (Stefan Visscher en Marieke Hermsen)
- Helpdesk Digitale Zorg (Merlijne Sonneveld)
- IZA-tafel (John Rijsdijk, Pascale Ooms en Chris Flim)
- KNMG (Sjaak Nouwt en Willemijn Put)
- KPN (Daan van Dooren, Cefas Dam en Harm Roosendaal)
- Landelijke Huisartsen Vereniging (LHV)
- Leiden University Medical Center (LUMC)/ National eHealth Living Lab (NeLL) (Niels Chavannes)
- Logius
- Luscii (Daan Dohmen en Derek Tersmette)
- Minddistrict (Jeanette Ploeger en Remy Lamers)
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Volksgezondheid, Welzijn en Sport
- NVZ-Ziekenhuizen (Lex Pater)
- OIZ (Yvonne Hoogendoorn)
- Patiëntenfederatie Nederland (Marcel Heldoorn)
- René van den Assem
- Yivi (voorheen Irma) (Bart Jacobs)
- Zorgthuisnl (Tonko Wedda)

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