Ministerie van Volksgezondheid,
Welzijn en Sport

Digitale toegang in de Zorg

Beslisboom:
betrouwbaarheidsniveaus en erkende inlogmiddelen

Verder

Beslisboom:
betrouwbaarheidsniveaus en erkende inlogmiddelen

Welke eisen zijn voor uw situatie van toepassing?

Een video-afspraak met een arts, een horloge dat de hartslag bijhoudt, digitale portalen waarop patiënten hun gezondheidsdossier kunnen raadplegen; het zijn vormen van e-health die steeds vaker worden gebruikt.

Nu we ook in de zorg steeds meer online doen, wisselen zorgaanbieders ook steeds meer informatie digitaal uit met patiënten. Vaak gaat het om persoonlijke, privacygevoelige gegevens. Veiligheid staat voorop. Nu, en in de toekomst.
Als overheid zorgen we ervoor dat burgers veilig kunnen inloggen bij publieke dienstverleners, waaronder ook de zorg. Zo zijn medische gegevens goed beschermd.

Daarom stelt de overheid stapsgewijs hogere eisen aan de inlogmiddelen die zorgaanbieders gebruiken om patiënten toegang te bieden tot hun digitale diensten.

Welk betrouwbaarheidsniveau van toepassing is en of het gebruik van erkende inlogmiddelen verplicht is, hangt af van het type organisatie, de diensten die u levert en de gegevens die u verwerkt .

Dit document helpt te bepalen welke eisen voor u(w organisatie) van toepassing zijn.

Overzicht *relevante* wetgeving

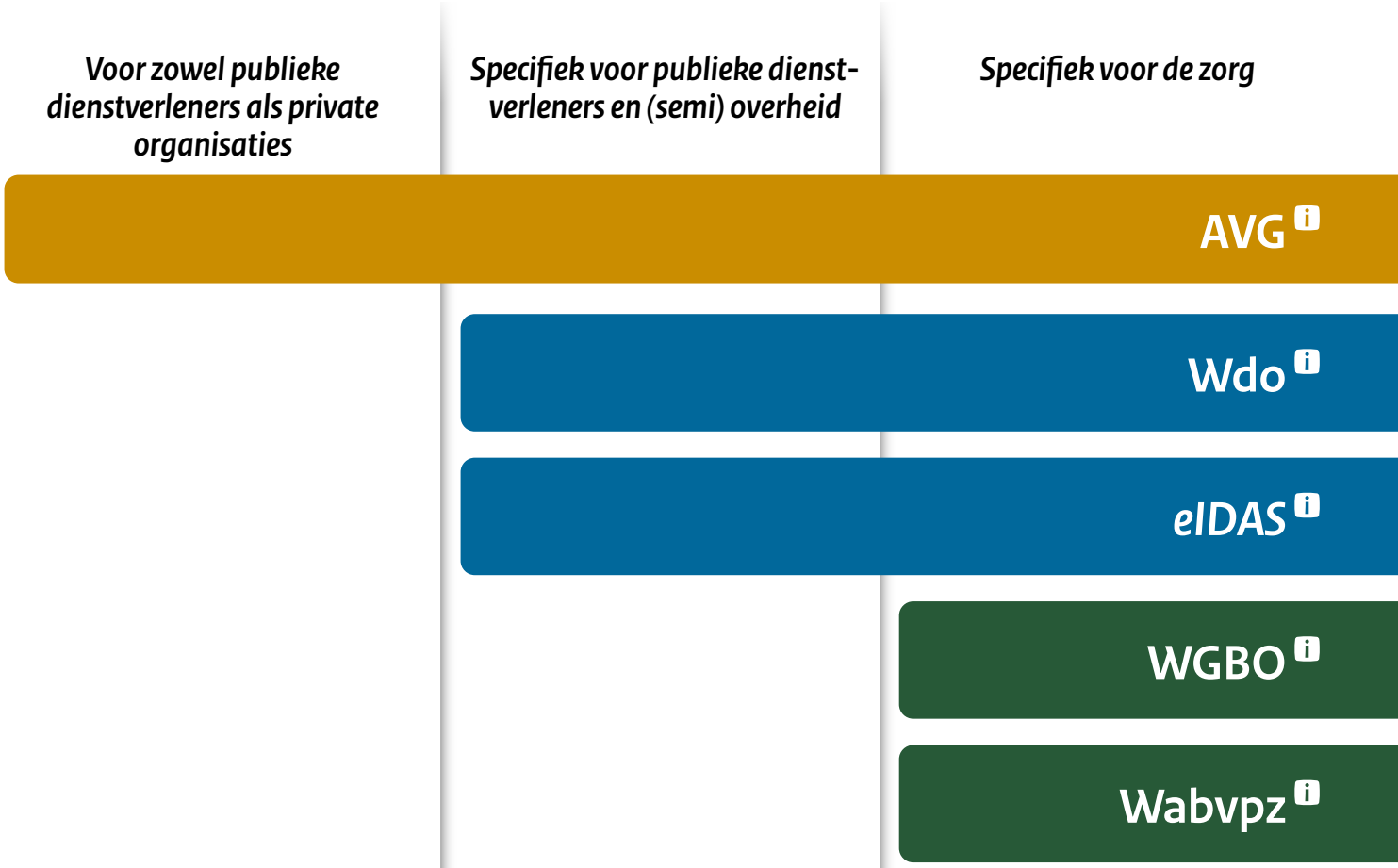
Met als scope veilige digitale toegang voor patiënten

In dit overzicht treft u de relevante wetgeving die richting geeft aan hoe u de digitale toegang voor uw patiënten inricht. We maken hierin onderscheid in drie typen wetten:

1. Wetten voor zowel publieke dienstverleners als private organisaties
2. Wetten voor publieke dienstverleners en (semi) overheid
3. Wetten specifiek voor het zorgdomein

Als zorgaanbieder zijn al de genoemde wetten van toepassing. Sommigen zijn al van kracht, anderen nog niet of nog niet voor iedereen.

Klik op de ⓘ voor meer informatie over die wet.



Beslisboom

Klik op de ℹ voor meer informatie

START

Ik ben:

Zorgaanbieder ℹ

Erkende inlogmiddelen: *gebruik verplicht*

Vallen de gegevens onder de **medische geheimhoudingsplicht?**

Ja → Betrouwbaarheidsniveau: **HOOG** ℹ

Nee → Betrouwbaarheidsniveau: **SUBSTANTIEEL** ℹ

Geen zorgaanbieder ℹ

Erkende inlogmiddelen: *gebruik erkende private inlogmiddelen is niet verplicht, maar wel toegestaan*

Is sprake van **geheimhoudingsplicht?**

Ja → Betrouwbaarheidsniveau: **HOOG** ℹ

Nee → Verwerkt u **bijzondere persoonsgegevens?**

Ja → Betrouwbaarheidsniveau: **SUBSTANTIEEL** ℹ

Nee → Verwerkt u **niet bijzondere persoonsgegevens?**

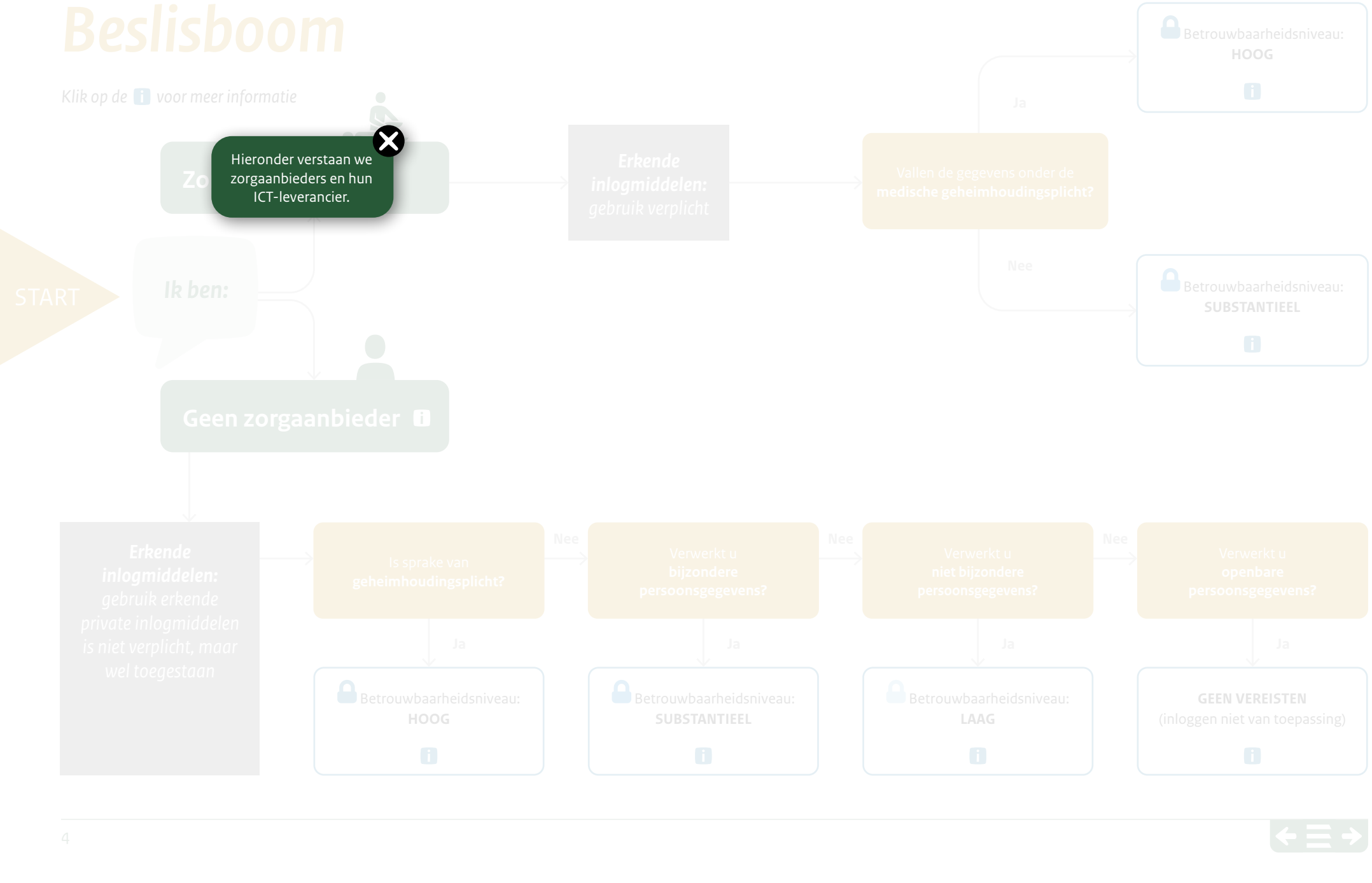
Ja → Betrouwbaarheidsniveau: **LAAG** ℹ

Nee → Verwerkt u **openbare persoonsgegevens?**

Ja → **GEEN VEREISTEN** (inloggen niet van toepassing) ℹ

Beslisboom

Klik op de ⓘ voor meer informatie



Beslisboom

Klik op de ℹ voor meer informatie

START

Ik ben:

Zorgaanbieder ℹ

Erkende inlogmiddelen: *gebruik verplicht*

Vallen de gegevens onder de **medische geheimhoudingsplicht?**

Ja → Betrouwbaarheidsniveau: **HOOG** ℹ

Nee → Betrouwbaarheidsniveau: **SUBSTANTIEEL** ℹ

Iemand anders

Hieronder verstaan we alle partijen die zelf geen zorgaanbieder zijn of onder de verantwoordelijkheid vallen van een zorgaanbieder.

Erkende inlogmiddelen: *gebruik erkende private inlogmiddelen is niet verplicht, maar wel toegestaan*

Is sprake van **geheimhoudingsplicht?**

Ja → Betrouwbaarheidsniveau: **HOOG** ℹ

Nee → Verwerkt u **bijzondere persoonsgegevens?**

Ja → Betrouwbaarheidsniveau: **SUBSTANTIEEL** ℹ

Nee → Verwerkt u **niet bijzondere persoonsgegevens?**

Ja → Betrouwbaarheidsniveau: **LAAG** ℹ

Nee → Verwerkt u **openbare persoonsgegevens?**

Ja → **GEEN VEREISTEN** (inloggen niet van toepassing) ℹ

Wabvpz

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg

Doel: *voor patiënten waarborgen creëren voor elektronische gegevensuitwisseling.*

Relevant in dit kader: *zorgverleners zijn verplicht patiënten inzage te bieden via elektronische weg.*

Voor wie van toepassing: *voor alle zorgverleners.*

Consequentie: *omdat toegang nu ook digitaal mogelijk moet zijn, neemt de hoeveelheid informatie die digitaal wordt uitgewisseld ook sterk toe. Dat vraagt om adequate beveiligingsmaatregelen.*

Wat maakt het actueel: *een deel van de Wabvpz is per 1 juli 2017 in werking getreden en een deel is sinds 1 juli 2020 van kracht. Zorgaanbieders zijn verplicht deze dienst te leveren en daarmee ook gehouden aan de andere wetten die toezien op de veiligheid van de toegang tot deze diensten.*

WGBO

Wet geneeskundige behandelingsovereenkomst

Doel: *regelt de rechten en plichten van patiënten die een geneeskundige behandelingsovereenkomst sluiten. Een belangrijk aspect daarin is de kwaliteit van de zorgverlening.*

Relevant in dit kader: *zorgverleners zijn verplicht een dossier aan te maken en hierin alle informatie op te slaan die nodig is voor het bieden van goede hulpverlening. De zorgverlener is verplicht tot geheimhouding (medische geheimhoudingsplicht) van dit medisch dossier en verplicht patiënten hier kosteloos toegang toe te bieden.*

Voor wie van toepassing: *voor alle zorgverleners.*

Consequentie: *om geheimhouding te waarborgen is adequate beveiliging van het medisch dossier noodzakelijk.*

Wat maakt het actueel: *nu patiënten recht hebben op digitale toegang tot dit dossier, zijn aanvullende maatregelen vereist om hen op veilige manier toegang te bieden.*

eIDAS

Electronic Identities And Trust Services

De Europese lidstaten hebben afgesproken dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken.

Doel: *het gebruik van grensoverschrijdende digitale dienstverlening bij publieke dienstverleners vergemakkelijken.*

Relevant in dit kader: *Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. Oftewel: met erkende inlogmiddelen van andere lidstaten kunnen inloggen bij publieke dienstverleners in Nederland en andersom. Dit kan alleen met een betrouwbare online identiteitscheck aan de voordeur.*

Voor wie van toepassing: *binnen de zorg is de eIDAS verordening vooralsnog alleen verplicht voor academische ziekenhuizen en zorgverzekeraars.*

Consequentie: *partijen die gehouden zijn aan deze verordening moeten – naast een inlogmiddel voor Nederlandse burgers – ook faciliteren dat burgers uit andere EU-lidstaten met een door dat lidstaat erkend inlogmiddel gebruik kunnen maken van digitale zorgdiensten.*

Wat maakt het actueel: *de eIDAS verordening is sinds 2018 van kracht en daarmee een verplichting waaraan moet worden voldaan. De betrouwbaarheidsniveaus zoals in de eIDAS verordening zijn opgenomen, worden ook in de AVG en Wdo toegepast en luiden als volgt:*

GROEIPAD BETROUWBAARHEIDSNIVEAUS	
LAAG (*gebruikersnaam + wachtwoord*)	✓
LAAG (*2-factor authenticatie via sms of DigiD app*)*	✓
SUBSTANTIEEL (*DigiD app + eenmalige ID-check*)	✓
HOOG (*DigiD app + terugkerende ID-check*)	

Wdo

Wet digitale overheid

Doel: *het regelen van veilig en betrouwbaar inloggen bij de (semi-)overheid.*

Relevant in dit kader: *de Wdo stelt onder andere het gebruik van door de overheid erkende inlogmiddelen verplicht. Daarnaast is sprake van een acceptatieplicht voor alle erkende inlogmiddelen en moet de informatiebeveiliging op orde zijn. Voor wie van toepassing: voor alle organisaties die kunnen worden aangemerkt als 'zorgaanbieder'.*

Consequentie: *alleen erkende inlogmiddelen mogen worden gebruikt. Op dit moment is dat alleen DigiD, maar op termijn kunnen ook private inlogmiddelen worden erkend. Als zorgaanbieder ben je verplicht ALLE erkende inlogmiddelen te ondersteunen.*

Wat maakt het actueel: *de Wdo ligt ter goedkeuring voor bij de Eerste Kamer. Het is verstandig tijdig voorbereidingen te treffen om aan deze nieuwe richtlijnen te voldoen.*

Erkende inlogmiddelen op betrouwbaarheidsniveau HOOG:

GROEIPAD WET DIGITALE OVERHEID
IN WERKINGTREDING WDO
ERKENNING VAN PRIVATE INLOGMIDDELEN
IMPLEMENTATIE ZORGAANBIEDERS
GEBRUIK DOOR PATIËNTEN

AVG

Algemene verordening gegevensbescherming

Doel: *privacy van burgers waarborgen.*

Relevant in dit kader: *de Autoriteit Persoonsgegevens, de toezichthouder in het kader van de AVG, heeft gesteld dat medische informatie op het hoogst breed beschikbare betrouwbaarheidsniveau moet worden beschermd.*

Voor wie van toepassing: *voor alle organisaties die medische gegevens opslaan. Los van de vraag wie de betreffende informatie beheert.*

Consequentie: *technische ontwikkelingen bieden steeds meer mogelijkheden voor de bescherming van medische gegevens en het bieden van veilige digitale toegang. Van de zorgsector wordt verlangd dat ze het hoogste breed beschikbare betrouwbaarheidsniveau gebruiken. De norm daarin zal de komende jaren verder stijgen.*

Wat maakt het actueel: *steeds meer patiënten beschikken over authenticatiemiddelen op een hoger niveau dan een combinatie tussen gebruikersnaam/wachtwoord of 2-factor authenticatie. Zo heeft al een flink deel van alle DigiD gebruikers in Nederland een eenmalige ID-check gedaan in de app. Daarmee beschikken zij over DigiD op niveau substantieel (een niveau hoger dan de 2-factor authenticatie van DigiD). Dit aantal stijgt maandelijks en zodra de Autoriteit Persoonsgegevens oordeelt dat dit niveau 'breed beschikbaar' is, kan van de zorgsector geëist worden dat zij dit niveau gaan toepassen in hun authenticatieprocessen.*

Erkende inlogmiddelen + betrouwbaarheidsniveau hoog

Voorbeeld

Een patiënt vult een vragenformulier in via een online platform, als onderdeel van zijn/haar behandeling.

Toelichting:

U geeft aan zorgaanbieder te zijn (of uw klant is dat). In dat geval is onder de Wet digitale overheid het **gebruik van erkende inlogmiddelen verplicht**. Informatie die tussen een patiënt en een zorgaanbieder wordt uitgewisseld in het kader van de behandelrelatie valt onder het medisch beroepsgeheim. Voor informatie die valt onder het medisch beroepsgeheim geldt betrouwbaarheidsniveau hoog. Het maakt hierbij niet uit wat de drager van de informatie is (tekstdocument, online vragenlijst, foto, video). Dat betekent dat voor deze situatie **betrouwbaarheidsniveau HOOG** van toepassing is. Op dit moment zijn de (eIDAS) betrouwbaarheidsniveaus laag en substantieel beschikbaar. Op termijn wordt ook niveau hoog bruikbaar. Daarnaast zijn er naast DigiD nog geen andere - private - inlogmiddelen erkend. Dit in afwachting van de Wdo.

GROEIPAD BETROUWBAARHEIDSNIVEAUS	
LAAG (*gebruikersnaam + wachtwoord*)	✓
LAAG (*2-factor authenticatie via sms of DigiD app*)*	✓
SUBSTANTIEEL (*DigiD app + eenmalige ID-check*)	✓
HOOG (*DigiD app + terugkerende ID-check*)	

Huidige stand van zaken:

DigiD Hoog is nog niet breed beschikbaar. Zo zijn bijvoorbeeld nog niet alle identiteitsbewijzen uitgerust met de benodigde chip. Het gebruik van deze variant van DigiD wordt verplicht zodra het is aangemerkt als 'breed beschikbaar' onder het publiek. Tot die tijd richten we ons op het niveau daaronder: DigiD Substantieel.

Vergelijkbare voorbeelden:

- Online een afspraak inplannen bij zijn/haar behandelaar.
- Online medicatieoverzicht inzien.
- E-consult/online chat/online behandeling via het patiëntenplatform van de zorgaanbieder.
- Online gegevens inzien/muteren in het medisch dossier via het patiënten portaal.
- Online gegevens invullen in een PGO en deze uploaden naar de zorgaanbieder.
- Via een PGO verbinding maken met het dossier bij de zorgaanbieder en (delen van) deze informatie downloaden om in het PGO op te slaan.
- Via telemonitoring de gezondheid van een patiënt bewaken. De patiënt gebruikt eigen hardware om de gegevens digitaal aan de zorgaanbieder te sturen.
- Online informatie (over de behandeling van een patiënt) aanbieden via het patiëntenportaal.

* *Bij de eIDAS betrouwbaarheidsniveaus is ook 2-factor authenticatie aangemerkt als niveau laag.*

Erkende inlogmiddelen + betrouwbaarheidsniveau substantieel

Voorbeeld

Een patiënt maakt online een afspraak bij zijn/haar huisarts en vult hiervoor zijn NAW-gegevens in.

Toelichting:

U geeft aan zorgaanbieder te zijn (of uw klant is dat). In dat geval is onder de Wet digitale overheid het **gebruik van erkende inlogmiddelen verplicht**.
Omdat hier geen sprake is van gegevens die gerelateerd zijn aan de behandeling van de patiënt is er wel sprake van geheimhoudingsplicht, maar is het medisch beroepsgeheim niet van kracht. Dat betekent dat voor deze situatie **betrouwbaarheidsniveau Substantieel** van toepassing is.
Op dit moment zijn de (eIDAS) betrouwbaarheidsniveaus laag en substantieel beschikbaar. Op termijn wordt ook niveau hoog beschikbaar gesteld.
Daarnaast zijn er naast DigiD nog geen andere - private - inlogmiddelen erkend. Dit in afwachting van de Wdo.

GROEIPAD BETROUWBAARHEIDSNIVEAUS	
LAAG (*gebruikersnaam + wachtwoord*)	✓
LAAG (*2-factor authenticatie via sms of DigiD app*)*	✓
SUBSTANTIEEL (*DigiD app + eenmalige ID-check*)	✓
HOOG (*DigiD app + terugkerende ID-check*)	

Huidige stand van zaken:

Het gebruik van DigiD Substantieel onder burgers neemt sterk toe en stijgt maandelijks. Al een aanzienlijk deel van hen heeft de DigiD app gedownload en hierin de eenmalige ID-check gedaan. Daarmee beschikken zij over DigiD Substantieel.

Vergelijkbare voorbeelden:

- Alle andere situaties waarin niet-medische gegevens worden verwerkt. Denk aan geboortedatum, mailadres, telefoonnummer.

* *Bij de eIDAS betrouwbaarheidsniveaus is ook 2-factor authenticatie aangemerkt als niveau laag.*

Geen erkende inlogmiddelen

U geeft aan geen zorgaanbieder te zijn, maar – bijvoorbeeld – een aanbieder van een PGO. In dat geval is het gebruik van erkende inlogmiddelen niet verplicht. U kunt gebruikmaken van private erkende inlogmiddelen. U kunt geen gebruikmaken van DigiD omdat u niet gerechtigd bent het BSN van uw klanten te verwerken.

Ook als het gebruik van door overheid ontwikkelde erkende inlogmiddelen niet verplicht is, kan wel sprake zijn van een verplicht betrouwbaarheidsniveau. Er zijn – afhankelijk van de situatie – vier mogelijkheden:

- Hoog betrouwbaarheidsniveau
- Substantieel betrouwbaarheidsniveau
- Laag betrouwbaarheidsniveau
- Geen sprake van inloggen, dus vereisten niet van toepassing.

Als er sprake is van uitwisseling van persoonsgegevens die gerelateerd zijn aan iemands gezondheid, dan geldt daar een geheimhoudingsplicht op en is **betrouwbaarheidsniveau hoog** van kracht.

Als het gaat om informatie die niet wordt uitgewisseld met een zorgaanbieder in het kader van de medische status van een persoon (of mogelijk zelfs geen betrekking op de persoon zelf heeft zoals wanneer een patiënt informatie opslaat in een PGO over bepaalde aandoeningen), dan is de geheimhoudingsplicht niet van kracht. Als er daarnaast geen bijzondere persoonsgegevens worden verwerkt, maar bijvoorbeeld alleen naam, adres, woonplaats, mailadres, etc. dan is het **betrouwbaarheidsniveau laag** van toepassing.

Er zijn ook situaties denkbaar waar **geen vereisten** zijn wat betreft het betrouwbaarheidsniveau. Wanneer er alleen openbare persoonsgegevens worden verwerkt, dan is inloggen geen vereiste. De betrouwbaarheidsniveaus zoals in dit document zijn toegelicht, zijn daarom niet van toepassing.

Private inlogmiddelen

Private inlogmiddelen kunnen de markt betreden zodra zij erkend zijn onder de Wet digitale overheid. Daarnaast kunnen andere inlogmiddelen ook gebruikt worden, als die aan de hoogst beschikbare betrouwbaarheidsniveaus voldoen. Op dit moment is dat nog 2-factor authenticatie.

Voor meer informatie over de vereisten die aan inlogmiddelen worden gesteld op verschillende niveaus verwijzen wij u naar het Forum voor Standaardisatie.

Colofon

Publicatie van Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid

mei 2022

Dit document geeft een versimpelde weergave van het juridisch kader; er kunnen geen rechten aan worden ontleend.