AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Ministerie van Volksgezondheid, Welzijn en Sport
t.a.v. de secretaris-generaal
Directie Wetgeving en Juridische Zaken (cluster 6)
Parnassusplein 5
2511 VX DEN HAAG

Datum	Ons kenmerk	Uw brief van
4 oktober 2018	z2018-17577	26 juli 2018
	Contactpersoon	Uw kenmerk

Onderwerp
Patiëntauthenticatie

Geachte,

Bij brief van 26 juli 2018 hebt u bij de Autoriteit persoonsgegevens (AP) aandacht gevraagd voor patiëntauthenticatie bij digitale informatie-uitwisseling tussen zorgaanbieders en patiënten. In uw brief geeft u aan dat in het zorgveld opnieuw vragen zijn ontstaan over welk niveau van patiëntauthenticatie op dit moment gebruikt dient te worden voor het uitwisselen van medische gegevens tussen zorgverleners en patiënten. In reactie op uw brief bericht de AP u als volgt.

1 Algemeen

Innovatieve technologie in de gezondheidszorg is goed...

De komende jaren neemt het aanbod van onlinedienstverlening in de zorg verder toe. Doel daarvan is dat de patiënt meer toegang tot en regie over de eigen medische gegevens krijgt. De AP staat in beginsel positief tegenover deze technologische ontwikkelingen. Die kunnen namelijk bijdragen aan kwalitatief goede, veilige en doelmatige patiëntenzorg.

... mits de privacy van patiënten is gewaarborgd

Bij technologische ontwikkelingen in de zorg moet er wel rekening worden gehouden met de bescherming van persoonsgegevens van patiënten. Gegevens over gezondheid zijn per definitie privacygevoelig. 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.

Datum
4 oktober 2018

Ons kenmerk
z2018-17577

Elektronische uitwisseling van gegevens over gezondheid tussen artsen en patiënten, zoals persoonlijke gezondheidsomgevingen en patiëntportalen, zijn pas mogelijk als gebruik wordt gemaakt van inlog- en identificatiemethoden met een passend betrouwbaarheidsniveau. De betrouwbaarheid van elektronische identificatiemiddelen wordt onder meer bepaald door de koppeling tussen persoonsidentificatiegegevens met de persoon, het uitgifteproces van een elektronisch identificatiemiddel, het beheer van het middel, de gebruikte techniek en de inrichting van het authenticatieproces.

2 Passende technische en organisatorische maatregelen

Wat zegt de AVG?

Op grond van artikel 32 AVG moeten verwerkingsverantwoordelijken en verwerkers passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Naarmate de persoonsgegevens een gevoeliger karakter hebben of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekent, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Gegevens over gezondheid zijn per definitie gevoelig, dus worden hoge eisen gesteld aan de beveiliging van die gegevens.

Wanneer is een beveiligingsmaatregel "passend"?

Er kunnen geen algemene uitspraken worden gedaan over wat een "passende" beveiligingsmaatregel is. Dat is afhankelijk van de concrete omstandigheden van het geval. Bij de uitleg van het begrip "passend" zoekt de AP aansluiting bij algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de *Code voor Informatiebeveiliging* of de *ICT-Beveiligingsrichtlijnen voor webapplicaties* van het Nationaal Cyber Security Centrum. Daarnaast zijn concrete normen voor informatiebeveiliging opgenomen in de ISO/NEN 27001 en 27002. Voor wat betreft de zorgsector (verwerking van gegevens over gezondheid) zijn deze normen uitgewerkt in NEN 7510:2017 en in aanvulling daarop NEN 7512:2015 en NEN 7513:2018. De AP ziet die normen als een beveiligingsstandaard die binnen de sector algemeen wordt geaccepteerd en die organisaties binnen de zorgsector moeten toepassen.

De eIDAS-verordening

De Europese eIDAS-verordening[1] gaat over de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt. Het leidt tot een wettelijk kader voor betrouwbaarheidsniveaus. Europese burgers en bedrijven moeten vanaf 29 september 2018 bij alle Nederlandse organisaties in de publieke sector kunnen inloggen met een door Europa erkend nationaal inlogmiddel. Om het betrouwbaarheidsniveau van online inloggen te verhogen, werkt de overheid aan een set van afspraken voor elektronische identificatie en authenticatie, het zogenaamde eID-stelsel.[2] De AP heeft dit belang met grote nadruk onderschreven.[3] Bij brief van 16 juli 2018 heeft de staatsecretaris van Binnenlandse Zaken en Ko-

[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.
[2] *Kamerstukken II* 2016-2017, 26 643, nr. 476.
[3] Brief van de AP aan de minister van BZK van 14 september 2016, met kenmerk z2015-00357.

ninkrijksrelaties de Tweede Kamer geïnformeerd over de voortgang van het programma eID en over de implementatie van de eIDAS-verordening.[4]

3 Toepasselijke norm voor patiëntidentificatie in de zorg

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.[5] 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. Dit is in lijn met de conclusies van een onderzoek uit 2016, dat op verzoek van het ministerie van VWS is uitgevoerd door de advieskantoren PBLQ en Privacy-Care. De minister van VWS heeft deze conclusies destijds gedeeld met de Tweede Kamer.[6] In de brief schreef de minister dat de conclusies uit het rapport de leidraad zullen zijn bij de invulling van de eisen waaraan authenticatiemiddelen in de zorg moeten voldoen.

4 Wat te doen zolang de vereiste betrouwbaarheidsniveaus nog niet breed beschikbaar zijn?

Probleem: nog geen brede beschikbaarheid

De AP is zich ervan bewust dat patiëntauthenticatie op betrouwbaarheidsniveaus "substantieel" en "hoog" op dit moment (nog) niet breed beschikbaar is als gebruik wordt gemaakt van DigiD. De staatssecretaris van BZK heeft in de eerder genoemde brief aan de Tweede Kamer 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. Volgens de staatssecretaris is *"het betrouwbaarheidsniveau "substantieel", in combinatie met publieke en één of meerdere (nog te verwerven) private authenticatiediensten, wél gereed voor bredere implementatie"*.

Uitgangspunt van de AP

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 on voldoende 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.

[4] *Kamerstukken II* 2017-2018, 26 643, nr. 550.
[5] Zie de brief van de AP aan de NVZ Nederlandse Vereniging van Ziekenhuizen van 7 oktober 2016.
[6] Brief van 4 november 2016, *Kamerstukken II* 2016-2017, 27 529, nr. 143.

Datum
4 oktober 2018

Ons kenmerk
z2018-17577

Wat te doen in de tussentijd?

Brede beschikbaarheid van betrouwbaarheidsniveaus “substantieel” en “hoog” voor alle patiënten zal nog enige tijd in beslag nemen. Het zou niet goed zijn – en ook niet in het belang van de patiënt – als zorginnovaties stilstaan totdat die betrouwbaarheidsniveaus binnen het eID-programma breed beschikbaar zijn. 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. Dat past ook bij de hiervoor aangehaalde uitgangspunten van de staatssecretaris van BZK.

Verder moet de zorgsector bezien welke mogelijkheden – eventueel buiten DigiD om – momenteel wél beschikbaar zijn om te gebruiken voor patiëntauthenticatie. Zo zijn er binnen de gezondheidszorg enkele pilots uitgevoerd, zoals het Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional (VIPP) en het MedMij-programma.[7] Het is van belang dat op basis daarvan op zo kort mogelijke termijn wordt geëvalueerd of de nieuwe middelen op niveau “substantieel” en “hoog” werken zoals beoogd. 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.

Tot slot: naar een toekomstbestendige manier van patiëntauthenticatie

Tot slot vraagt de AP u te bevorderen dat binnen de zorgsector wordt geïnvesteerd in een toekomstbestendige wijze van patiëntidentificatie op een passend betrouwbaarheidsniveau. Een passend beveiligingsniveau is immers mede afhankelijk van de stand van de techniek. Die techniek staat niet stil. Dat betekent dat de wijze van patiëntidentificatie technisch flexibel moet zijn, zodat snel en eenvoudig nieuwe en/of aanvullende beveiligingsmaatregelen kunnen worden getroffen wanneer de stand van de techniek dat vereist.

Hoogachtend,
de Autoriteit persoonsgegevens,
w.g.

mr. A. Wolfsen
voorzitter

[7] Zie nader ”Het nieuwe eID-stelsel; een introductie voor de zorgsector”, Nictiz: mei 2017.