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

Bestuur Nederlandse Vereniging Ziekenhuizen

Datum
7 oktober 2016

Contactpersoon

Onderwerp
Twee-factor authenticatie van patiënten bij toegang patiëntportals

Geachte heer, mevrouw,

Naar aanleiding van door Nictiz[1] gepubliceerde onderzoeksresultaten over de beschikbaarheid van zogenaamde patiëntportals bij ziekenhuizen, signaleert de Autoriteit Persoonsgegevens (AP) een punt van zorg waarvoor de AP uw aandacht wil vragen.

In dit Nictiz-onderzoek wordt aangegeven dat van de momenteel bij 22 ziekenhuizen functionerende patiëntportals er bij slechts 12 van die patiëntportals een systeem wordt gehanteerd waardoor de patiënt toegang krijgt tot zijn/haar gegevens na een twee-factor authenticatie (DigiD en SMS). Bij 5 patiëntportals zou sprake zijn van het kunnen inloggen met uitsluitend DigiD en van 5 patiëntportals wordt niet vermeld op welke andere wijze het inloggen mogelijk wordt gemaakt.

In uitspraken en richtsnoeren heeft de AP regelmatig aangegeven dat bij de patiënt-authenticatie 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.

[1] www.nictiz.nl/SiteCollectionDocuments/Infographics/Factsheet%20pati%c3%abntportalen%20ziekenhuiswebsites_update.pdf

Datum
7 oktober 2016

De AP is zich ervan bewust dat patiënt-authenticatie op betrouwbaarheidsniveau 'hoog' (STORK niveau 4) op dit moment (nog) niet breed beschikbaar is.
In afwachting van het breder beschikbaar komen van een authenticatiemethode van een passend hoog niveau, acht de AP het evenwel niet aanvaardbaar dat ziekenhuizen bij de inrichting van patiëntportals afzien van gebruik van de al wel bestaande mogelijkheden tot twee-factor authenticatie van patiënten (zoals DigiD in combinatie met SMS).
Uitgaand van de bevindingen in het onderzoek van Nictiz zouden vooralsnog 10 ziekenhuizen bij de toegang tot patiëntportals niet voorzien in patiënt-authenticatie op het vereiste betrouwbaarheidsniveau, hetgeen in strijd is met artikel 13 Wbp.

De AP vraagt uw aandacht voor deze kwestie en verzoekt u om op passende wijze bij uw leden onder de aandacht te brengen dat zij gehouden zijn om bij de toegang tot patiëntportals een wijze van patiënt-authenticatie te hanteren die voldoet aan het op grond van artikel 13 Wbp vereiste betrouwbaarheidsniveau. Minimaal voorzien in gebruik van de bestaande mogelijkheden tot twee-factor authenticatie is de norm waaraan dient te worden voldaan.
Op bureauniveau zal door de AP contact worden opgenomen om over de wijze van informeren van uw leden verder van gedachten te wisselen.

De AP gaat er vanuit de ziekenhuizen die nu nog geen gebruik maken van de bestaande mogelijkheden tot twee-factor authenticatie van patiënten met de benodigde voortvarendheid hun handelwijze zullen aanpassen. Alsdan zal de inzet van handhavende maatregelen door de AP niet aan de orde hoeven komen.

Hoogachtend,
De Autoriteit Persoonsgegevens,

mr. W.B.M. Tomesen
Vice-voorzitter