Uniforme maatregel 09 - Gebruik authenticatiemiddelen bij internetapplicaties

Inhoudsopgave

Uniforme maatregel

Uniforme maatregel 09 - Gebruik authenticatiemiddelen bij internetapplicaties

Inhoud	Authenticatie-eisen voor internetapplicaties (waaronder apps) van zorgverzekeraars bij het verstrekken van online informatie aan verzekerden.
Versienummer	1
Status	Definitief
Kenmerk	UM-14-15-bjag1

AUTEUR
Mr. Ir. P.L.F. Algra

DATUM
17 mei 2014

1. Inleiding

Informatieverstrekking aan de consument vindt steeds vaker digitaal plaats. Zorgverzekeraars verwerken bijzondere persoonsgegevens die een bijzondere rechtsbescherming genieten en waarbij een hoog niveau van beveiliging vereist is. Informatieverstrekking vindt ook bij zorgverzekeraars steeds vaker digitaal plaats, waaronder via de 'mijn'-omgeving. In die omgeving kunnen ook declaratiegegevens getoond worden. De Wet bescherming persoonsgegevens (hierna: Wbp) beschouwt dit als bijzondere persoonsgegevens. Dit betekent dat aan de authenticatie specifieke eisen worden gesteld.

In deze Uniforme Maatregel (UM) wordt (op basis van de aard van de aan verzekerden getoonde gegevens en de daarbij behorende risicoklasse) inzichtelijk gemaakt aan welke eisen voldaan moet worden om de identiteit van de verzekerde vast te stellen.
Twee met elkaar samenhangende ontwikkelingen zijn de aanleiding voor deze UM:

1. Meer maatschappelijke aandacht voor beveiliging van websites.
2. Toezichthouders stellen meer eisen aan toegangsbeveiliging van websites van verzekeraars.

De UM past binnen de daarvoor geldende wettelijke kaders en is gebaseerd op twee kaderstellende rapporten:

1. CBP Richtsnoeren 'Beveiliging van persoonsgegevens' (hierna Richtsnoeren)[1];
2. Achtergrondstudies en Verkenningen 23 (hierna AV23)[2].

---

[1] In werking getreden op 1 maart 2013, zie http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

[2] G.W. van Warkom en J.J. Borking, Beveiliging van persoonsgegevens, Achtergrondstudies en Verkenningen 23, Registratiekamer, Den Haag, april 2001. (http://www.cbpweb.nl/Pages/av_23_Beveiliging.aspx). De Registratiekamer was de voorloper van het College Bescherming Persoonsgegevens. Hoewel dit normatieve advies uit 2011 stamt, is het nog steeds relevant en bruikbaar als norm voor het bepalen van de toepasselijke risicoklassen.

De Richtsnoeren leggen uit hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. De Richtsnoeren vormen de verbindende schakel tussen enerzijds het juridisch domein, met daarbinnen de eisen uit de Wbp, en anderzijds het domein van de informatiebeveiliging.

Uit AV23 zijn de risicoklasse-indeling en de beveiligingsmaatregelen gebruikt. Dit rapport is vervangen door de Richtsnoeren en daarmee niet langer het uitgangspunt voor onderzoek door het CBP. De inhoud is echter onveranderd relevant en bruikbaar voor een nadere invulling van de risico-analyse.

1.1 Doelstelling en bereik

Deze UM is opgesteld met als doel het formuleren van een passende minimumeis voor zorgverzekeraars aan de authenticatie van de verzekerde en/of verzekeringnemer (beiden hierna aangeduid als verzekerde). Deze authenticatie dient voorafgaand aan de toegang tot zijn persoonsgegevens middels internetapplicaties (waaronder apps) plaats te vinden.

1.2 Uitgangspunten en afwegingen

Bij het formuleren van de UM zijn drie belangrijke afwegingen meegenomen:

1. De maatregel moet waarborgen dat de gegevens van de verzekerde zo goed mogelijk beveiligd zijn en niet toegankelijk zijn voor een ander dan de verzekerde zelf (bij ieder type informatie een passend slot);
2. Tegelijkertijd dient de verzekerde op klantvriendelijke wijze toegang te krijgen tot zijn eigen gegevens (geen sleutelbos of keten van sloten indien dat niet nodig is) Hieraan is invulling gegeven door te kiezen voor een minimaal niveau van beveiliging, passend binnen relevante wet- en regelgeving;
3. Tenslotte is het van belang binnen de vigerende wet- en regelgeving uniformiteit te bereiken over de wijze waarop de wettelijke eisen die gelden voor de authenticatie van de verzekerde, worden ingevuld.

De veiligheid van de verzekerdengegevens, het gebruikersgemak voor de verzekerde en vigerende wet- en regelgeving zijn de basis geweest voor de UM. Deze afwegingen impliceren dat de beveiligingsmaatregelen getroffen moeten worden waar ze horen: lage risico's: lage drempels, hoge risico's: hoge drempels.
Belangrijk is dat de verzekerde de maatregel ervaart als een passende veiligheidsmaatregel ten behoeve van de bescherming van zijn persoonsgegevens. Aangezien internetapplicaties in toenemende mate als primaire bron van informatie worden gebruikt, is het van belang dat het gebruik hiervan niet wordt ontmoedigd .

Bij het opstellen van de UM werd DigiD door veel zorgverzekeraars gebruikt als middel voor toegangsbeveiliging. Andere zorgverzekeraars werken aan invoering van DigiD. Gebruik van DigiD heeft als voordeel dat de Nederlandse burger bekend is met het systeem (één manier van inloggen bij verschillende diensten) en dat het als overheidssysteem ook aan hoge veiligheidsnormen voldoet (betrouwbare overheidsdienstverlening).
De voordelen voor de zorgverzekeraar zijn daarbij evident: inrichten en beheren van identiteiten is uitbesteed en de koppeling met het Gemeentelijke Basisadministratie (GBA) borgt in belangrijke mate de juistheid en volledigheid van informatie.
DigiD past binnen de kaders van aan de nieuwe CBP Richtsnoeren 'Beveiliging van persoonsgegevens'. De eisen in de CBP Richtsnoeren spitsen zich toe op de authenticatie en legt de nadruk op een risicoanalyse en passende maatregelen gebaseerd op open normen met verwijzing naar de gangbare normenkaders, richtlijnen en best practices.

1.3 In werking per 1 april 2015

De uniforme maatregel geldt tot 1 april 2015 als aanbeveling. Vanaf 1 april 2015 is de UM een verplichting.

2 Risicoklassen en de daaraan te stellen eisen

In dit hoofdstuk wordt op basis van de aard van de gegevens en de daarbij behorende risicoklasse inzichtelijk gemaakt welke eisen vanuit de overheid gelden per risicoklasse.

2.1 Risicoklassen

AV 23 geeft een normatief kader voor de concrete invulling van maatregelen en procedures ten aanzien van de beveiliging van persoonsgegevens tegen verlies of tegen onrechtmatige verwerking. De studie is gebaseerd op het bepaalde in artikel 13 Wbp en geeft richting aan hoe de verantwoordelijke met de beveiliging van persoonsgegevens dient om te gaan en vormt daarmee een nadere invulling van de Wbp. Voor de initiële inschatting van de risicoklasse op basis van de aard van de gegevens, kan de volgende tabel gebruikt worden:[3]

Klasse	Aard van de gegevens
Geen persoons-gegevens	De gegevens zijn niet te herleiden tot geïdentificeerde of identificeerbare personen. Zorgverzekeraars: polisvoorwaarden en verzekerde pakketten.
Risicoklasse 0	Publiek. Openbare persoonsgegevens waarvan algemeen aanvaard is dat deze geen risico opleveren voor betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures en publieke internetsites.
Risicoklasse I	Basis. Beperkt aantal persoonsgegevens dat betrekking heeft op één type vastlegging, bijvoorbeeld een lidmaatschap, arbeidsrelatie of klantrelatie zolang deze niet gerekend kunnen worden tot de bijzondere persoonsgegevens. Zorgverzekeraars: polisgegevens, pakketgegevens.
Risicoklasse II	Verhoogd risico. Bijzondere persoonsgegevens als genoemd in art. 16 Wbp, of financieel-economische gegevens in relatie tot de betrokkene. Zorgverzekeraars: overzicht (soort) zorgverbruik in detail en financieel declaratieoverzicht.[4]
Risicoklasse III	Hoog risico. Gegevens van opsporingsdiensten, DNA databank, gegevens waar bijzondere, wettelijk bepaalde, geheimhoudingsplicht op rust, gegevens

[3] Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, een handreiking voor overheidsorganisaties van het Forum Standaardisatie, januari 2012, p. 23. (http://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_WEB.pdf)

[4] Zie UM03.

	die onder beroepsgeheim vallen (bv. medisch) in de zin van art. 9 lid 4, Wbp. Niet van toepassing op zorgverzekeraars

Tabel 1: indeling van de risicoklassen op grond van de aard van de gegevens

2.2 Eisen die gelden voor de risicoklassen

AV23[5] werkt de eisen die gelden voor de respectievelijke risicoklassen uit. Wanneer sprake is van een hogere risicoklasse, zijn de maatregelen van de voorgaande risicoklasse(n) tevens van toepassing. Risicoklasse 0 (Publiek niveau) kent geen eisen. Risicoklasse III is niet van toepassing, aangezien zorgverzekeraars dergelijke gegevens niet verwerken of vastleggen. De eisen voor Risicoklasse I en II, zoals vastgelegd in AV23, zijn als volgt:

Risicoklasse I: Basis niveau

1. De opzet van een logische toegangscontrole op informatiesystemen is zodanig dat alleen een functionaliteit kan worden gebruikt waarvoor uitdrukkelijk een bevoegdheid is verleend;
2. Bij de logische toegangscontrole wordt de identiteit en de authenticiteit van gebruikers vastgesteld door tenminste een gebruikersnaam en een wachtwoord;
3. Een wachtwoord is slechts gedurende een van te voren vastgestelde periode geldig. Bij wijziging van het wachtwoord wordt gecontroleerd of het oude en nieuwe wachtwoord niet gelijk zijn. Voor de hand liggende wachtwoorden zijn niet toegestaan. Tevens moeten er regels opgesteld zijn waarin is vastgelegd aan welke eisen een goed gekozen wachtwoord moet voldoen. Het systeem voor toegangscontrole moet hierop ook controleren. Het wachtwoord wordt nergens in leesbare vorm vastgelegd. In het systeem voor toegangscontrole worden de wachtwoorden voldoende beveiligd, bijvoorbeeld door een one-way-hashing encryptie-algoritme;
4. Het aantal keren dat een foutief wachtwoord kan worden ingevoerd, moet worden beperkt tot maximaal drie. Bij overschrijding hiervan wordt de toegang tot het systeem onder de betreffende identificatie volledig geblokkeerd. Slechts een hiertoe geautoriseerde functionaris is gerechtigd de geblokkeerde identificatie weer vrij te geven. Dit gebeurt conform een vastgestelde procedure nadat de afwijkingen zijn onderzocht.

In afwijking op de eisen 3 en 4 uit de AV23 geldt voor de verzekeraars die kiezen voor DigiD de invulling van deze eisen zoals DigiD die hanteert.

Risicoklasse II: Verhoogd risico

[5] AV 23, p. 44 e.v.

5. Bij het verkrijgen van toegang tot persoonsgegevens via een computernetwerk wordt de gebruiker nauwkeurig geïdentificeerd. Het bevoegd gebruik van de persoonsgegevens is afhankelijk van meer dan alleen de toegangscontrole door gebruikersnaam en wachtwoord in te voeren, maar bijvoorbeeld ook van het tijdstip en de apparatuur die gebruikt wordt om toegang te krijgen;
6. Bij het overschrijden van het toegestane aantal pogingen om toegang te krijgen wordt de verantwoordelijke terstond geïnformeerd, zodat deze actie kan ondernemen;
7. Elke poging (geslaagd of niet) om toegang te krijgen tot een informatiesysteem met persoonsgegevens wordt vastgelegd in een logbestand. Dit logbestand heeft een voldoende lange bewaartijd, zodat een analyse van bijzonderheden kan worden gemaakt en hierover kan worden gerapporteerd;
8. Bij het overdragen van bevoegdheden moet de rechtmatigheid ervan achteraf vastgesteld kunnen worden.

3. Maatregel

Zorgverzekeraars voldoen, uiterlijk per 1 april 2015 aan de algemene eisen zoals verwoord in paragraaf 2.2 en nader uitgewerkt voor zorgverzekeraars in tabel 2. Deze toepassing behelst tevens het product DigiD. DigiD is een product van Logius, dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

In tabel 2 is de verbinding zichtbaar gemaakt tussen de risicoklassen, de daaraan te stellen eisen en de keuze van de zorgverzekeraars voor de passende vorm van authenticatie.

Gelet op de bepalingen in de Wbp en CBP Richtsnoeren 'Beveiliging van persoonsgegevens' over passende maatregelen, moet de risicoanalyse en de analyse van de stand der techniek periodiek worden herhaald.

Met vriendelijke groet,
Zorgverzekeraars Nederland

P. H. van Holst-Wormser
Algemeen Directeur

Risico klasse	Authenticatie-methode	Minimumeisen (cumulatief) in lijn met eisen genoemd in hoofdstuk 2	Implementatievoorstel
0 Publiek	Geen		
I Basis	single factor; kenniskenmerk met aanvullende waarborgen	1. alleen toegang indien bevoegd. 2. minimaal gebruikersnaam en wachtwoord. 3. beperkte geldigheidsduur wachtwoord; complexiteitseis; geen vastlegging in leesbare vorm, beveiliging wachtwoord in systeem; 4. maximaal drie foutieve aanmeldpogingen, daarna blokkering; goede deblokkeringsprocedure.	- DigiD of geldigheidsduur wachtwoord maximaal 1 jaar; gebruikersnaam / complex wachtwoord (minimaal 8 karakters waaronder een cijfer en een leesteken, controle op historie- en woordenlijst); - laatste gebruik op een scherm; - historisch gebruik opvraagbaar; - deblokkeringsprocedure bevat logging en monitoring.
II Verhoogd risico	multi factor; kenniskenmerk en bezitskenmerk met beperkte zekerheid	5. toegang met meer dan alleen gebruikersnaam en wachtwoord; 6. bij overschrijding toegestane aantal foutieve aanmeldpogingen de verantwoordelijke informeren; 7. logging en monitoring van aanmeldpogingen (succes en foutief); 8. audit-trail van overdracht bevoegdheden.	- DigiD met sms of gebruikersnaam / complex wachtwoord aangevuld met één van de volgende opties: - eenmalig wachtwoord via sms - TAN lijst - apparaat kenmerk

Tabel 2: authenticatietabel: de verbinding tussen de risicoklassen en de keuze voor passende vorm van authenticatie