COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

Onderzoek naar de beveiliging van het online aanvragen van herhaalrecepten bij huisarts en apotheek

DATUM 10 juli 2013

1. Inleiding

Het College bescherming persoonsgegevens (CBP) constateert dat het in toenemende mate mogelijk is herhaalrecepten online, door middel van een (web-)aanvraagformulier[1], aan te vragen bij huisartsen en apotheken.

In het kader van het aanvragen van herhaalrecepten worden medische gegevens verwerkt. Medische gegevens behoren tot de categorie bijzondere persoonsgegevens in de zin van de Wet bescherming persoonsgegevens (Wbp). Dat betekent dat ingevolge artikel 13 Wbp hoge(re) eisen worden gesteld aan de technische en organisatorische maatregelen die de verantwoordelijke dient te treffen om deze gegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

In mei 2013 heeft het CBP door middel van een steekproef 150 websites van huisartsen en apotheken onderzocht waar via internet herhaalrecepten kunnen worden opgevraagd. Het CBP constateert dat bij 43 websites het online aanvraagformulier over een onbeveiligde verbinding wordt verzonden. Als gegevens via een onbeveiligde verbinding worden verzonden, kunnen derden de gegevens relatief eenvoudig 'oppikken' (meelezen), verwijderen en aanpassen. Gelet op dit risico en gezien de aard van de gegevens op het aanvraagformulier is bij deze 43 websites in dit opzicht geen sprake van een passend beveiligingsniveau en handelt de verantwoordelijke voor zo'n website in strijd met artikel 13 Wbp.

Van de 43 websites behoren er 19 toe aan huisartsenpraktijken, 6 aan apotheekhoudende huisartsen en 18 aan apotheken. De 43 websites hebben daarmee gezamenlijk een geschat potentieel bereik van ongeveer 250.000 patiënten.[2]

Doel en reikwijdte van het onderzoek
Het onderzoek is gericht op websites van huisartsen en apotheken waar patiënten door middel van een online aanvraagformulier herhaalrecepten kunnen aanvragen. In het bijzonder richt het onderzoek zich op de beantwoording van de volgende onderzoeksvragen:

- Wordt het online aanvraagformulier vanaf de browser van de PC van de patiënt (hierna: "browser") *met of zonder* SSL-verbinding verzonden?
- Wordt het online aanvraagformulier met de ingevulde medische gegevens naar een plek (hierna: "server") *met of zonder* SSL-verbinding verzonden?

Indien één of beide vragen worden beantwoord met '*zonder SSL-verbinding*' stelt het CBP vast dat huisartsen en apotheken onvoldoende beveiligingsmaatregelen hebben getroffen en daarmee in strijd handelen met artikel 13 Wbp.

[1] Het online aanvraagformulier bevat onder meer de naam, geboortedatum, emailadres en benodigde medicatie (en benodigde hoeveelheid) van de betreffende patiënt.
[2] Gemiddeld heeft een huisartsenpraktijk ongeveer 4200 ingeschreven patiënten (Nederlandse Zorgautoriteit, 5 september 2012: Praktijkkosten- en inkomensonderzoek huisartsenzorg); De gemiddelde openbare apotheek heeft een patiëntenpopulatie van 7.800 personen (Data en feiten 2009 (augustus 2009). Stichting Farmaceutische Kengetallen).

2. Juridisch kader

Artikel 13 Wbp vereist dat de verantwoordelijke 'passende' beveiligingsmaatregelen treft teneinde persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Bij de bepaling van hetgeen in dit geval als 'passende technische en organisatorische maatregelen' in de zin van artikel 13 Wbp moet worden beschouwd zijn de NEN 7512 norm en de ICT-Beveiligingsrichtlijnen voor webapplicaties als meetinstrument gebruikt.

De NEN 7512 norm is van toepassing op de elektronische communicatie in de zorg tussen zorgverleners en zorginstellingen onderling en met patiënten en cliënten, met zorgverzekeraars en andere partijen die bij de zorg betrokken zijn. In deze norm worden minimumeisen gesteld met betrekking tot de bron van de gegevens, het transportkanaal en de ontvanger van de gegevens. Ten aanzien van online uitwisseling van medische gegevens vereist de NEN 7512 dat de verbinding waarover de gegevens worden uitgewisseld "versleuteld" is.[3] Deze NEN-norm vormt een gezaghebbende sectorale uitwerking van artikel 13 Wbp; de in deze normen beschreven maatregelen worden door partijen uit het veld als adequaat gezien, en de Richtsnoeren beveiliging van persoonsgegevens van het CBP gaan er vanuit dat zo'n binnen de sector algemeen geaccepteerde beveiligingsstandaard door de verantwoordelijke wordt toegepast.[4]

Het vereiste dat de verbinding versleuteld moet zijn, wordt bevestigd in de ICT-Beveiligingsrichtlijnen voor webapplicaties. Ook dit is een algemeen geaccepteerde beveiligingsstandaard die volgens de Richtsnoeren beveiliging van persoonsgegevens van het CBP dient te worden toegepast. Maatregel B5-2 van de ICT-Beveiligingsrichtlijnen voor webapplicaties stelt dat indien (contact)formulieren online over een onversleutelde verbinding (http in plaats van https) worden verzonden, de mogelijkheid bestaat dat de ingevulde gegevens door derden onderschept kunnen worden. Door de verbinding richting de webapplicatie te versleutelen via SSL of TLS wordt voorkomen dat kwaadwillenden eenvoudig de verkeersstromen tussen cliënt en server kunnen inzien.[5]

3. Werkwijze en resultaten

In mei 2013 heeft het CBP door middel van een steekproef 150 websites van huisartsen en apotheken onderzocht waar via internet herhaalrecepten kunnen worden aangevraagd.

Het CBP constateert dat bij 43 websites het online aanvraagformulier zowel vanaf de browser als naar de server zonder SSL-verbinding wordt verzonden.

[3] NEN 7512, p. 15.
[4] CBP Richtsnoeren beveiliging persoonsgegevens, februari 2013.
[5] ICT-Beveiligingsrichtlijnen voor webapplicaties Deel 2 (januari 2012). Nationaal Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie, p. 104 – 105.

4. Conclusie

43 van de onderzochte huisartsen en apotheken hebben medische gegevens over een onbeveiligde verbinding verzonden en hebben daarmee onvoldoende beveiligingsmaatregelen getroffen. Daarmee handelen zij in strijd met artikel 13 Wbp.