COLLEGE BESCHERMING PERSOONSGEGEVENS

College bescherming persoonsgegevens

Onderzoek naar de verwerking van medicatiegegevens door Farmazorg BV te Nijmegen

Z2013-131

Rapport definitieve bevindingen

12 november 2013

SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft in 2012-2013 onderzoek gedaan naar toegangsbeveiliging en logging bij de uitwisseling van medicatiegegevens tussen twee apotheken in Ermelo en tussen twee apotheken in Nijmegen, waaronder Dienstapotheek Nijmegen.

Farmazorg BV is verantwoordelijke in de zin van de Wbp voor de gegevensverwerkingen bij Dienstapotheek Nijmegen en dient dus passende maatregelen te treffen tegen onbevoegde kennisneming. Bij de apotheek worden gegevens verwerkt waarop een bijzondere geheimhoudingsplicht rust, waardoor het hoogste beveiligingsniveau is vereist.

Dienstapotheek Nijmegen is deelnemer van de Stichting OZIS Rijk van Nijmegen. Met behulp van de door deze stichting beheerde Centrale Patiëntenindex (CPI) kan Dienstapotheek Nijmegen patiëntgegevens inzien van andere apothekers in de regio Nijmegen.

Informatiesystemen, die patiëntgegevens verwerken, behoren, ingevolge artikel 13 Wbp en de nadere invulling hiervan in de richtsnoeren van het CBP en in de toepasselijke NEN-normen, aan bepaalde eisen te voldoen ten aanzien van toegangsbeveiliging (in casu identificatie en authenticatie) en logging.

Volgens NEN 7510 en -7512 moet de authenticatie bestaan uit twee afzonderlijke kenmerken (twee-factor authenticatie). Op de apotheek wordt echter uitsluitend gebruik gemaakt van wachtwoorden.

Naar aanleiding van de voorlopige bevindingen heeft Farmazorg BV maatregelen getroffen om de geconstateerde overtreding van artikel 13

Wbp te beëindigen. Het CBP concludeert evenwel dat vooralsnog niet is aangetoond dat deze maatregelen afdoende zijn.

1. Inleiding

Het College bescherming persoonsgegevens (CBP) heeft in 2012-2013 onderzoek gedaan naar toegangsbeveiliging en logging bij de uitwisseling van medicatiegegevens tussen twee apotheken in Ermelo en tussen twee apotheken in Nijmegen.

Het CBP heeft voor dit onderzoek gekozen omdat eventuele overtredingen op dit punt veel burgers treffen. Voorts gaat het om verwerking van bijzondere persoonsgegevens, waarmee gezien de aard ervan extra voorzichtig moet worden omgegaan. Deze persoonsgegevens dienen daarom zeer goed te worden beveiligd.

Het onderzoek richt zich op beveiliging van de medische gegevens die door apothekers en eventuele andere zorgverleners onderling worden uitgewisseld. Hierbij is met name gekeken naar toegangsbeveiliging en logging van raadplegingen.

Eén van de onderzochte apotheken is Dienstapotheek Nijmegen (hierna ook wel: de apotheek). Dienstapotheek Nijmegen is deelnemer van de Stichting OZIS Rijk van Nijmegen. Met behulp van de door deze stichting beheerde Centrale Patiëntenindex (CPI) kan Dienstapotheek Nijmegen patiëntgegevens inzien van andere apothekers in de regio Nijmegen. Dit maakt dat toegangscontrole en logging niet alleen betrekking hebben op de gegevens van Dienstapotheek Nijmegen, maar ook op die van deze andere apotheken.

Op 4 maart 2013 heeft het CBP interviews gehouden met twee bestuurders van Farmazorg BV - de verantwoordelijke voor Dienstapotheek Nijmegen (zie verder p. 5) - en met een beherend apotheker. Ook werd door hen een demonstratie gegeven van de voor dit onderzoek relevante onderdelen van de gebruikte systemen. Tijdens dit onderzoek is schriftelijk bewijsmateriaal verkregen. Eerder werden op 3 december

2012 interviews gehouden met de voorzitter, de penningmeester en een in ICT gespecialiseerde deelnemer van de Stichting OZIS Rijk van Nijmegen.

Bij brief van 22 juli 2013 is het rapport voorlopige bevindingen naar Farmazorg BV verzonden. Farmazorg BV heeft op 6 augustus 2013 schriftelijk op deze voorlopige bevindingen gereageerd.

Wettelijk kader

Ingevolge artikel 1 onder d Wet bescherming persoonsgegevens (Wbp) is de verantwoordelijke de natuurlijke persoon, rechtspersoon of ieder ander die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Medische gegevens zijn bijzondere gegevens in de zin van artikel 16 Wbp. De verwerking daarvan is verboden tenzij -onder andere- deze ingevolge artikel 21, eerste lid onder a Wbp geschiedt door hulpverleners, instellingen of voorzieningen voor gezondheidszorg voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is.

In artikel 13 Wbp is bepaald dat de verantwoordelijke *passende technische en organisatorische maatregelen* ten uitvoer legt om persoonsgegevens te beveiligen tegen enige vorm van *onrechtmatige verwerking*. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van tenuitvoerlegging, een *passend* beveiligingsniveau garanderen, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich brengen.

Passend

In het begrip 'passend' ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. De wetgever heeft deze norm niet nader ingevuld omdat de

stand van de techniek sterk tijdgebonden is. Invulling van de norm zou afbreuk doen aan het nagestreefde niveau van beveiliging.
Het begrip 'passend' duidt mede op de proportionaliteit tussen beveiligingsmaatregelen en de aard van de te beschermen gegevens. Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens.[1] Gegevens betreffende de gezondheid worden aangemerkt als bijzondere ofwel gevoelige gegevens.[2]

Onrechtmatige verwerking

In artikel 7:457, lid 1, van het Burgerlijk Wetboek (BW) is bepaald dat de hulpverlener[3] geen inzage in of afschrift van bescheiden uit het medisch dossier verschaft aan anderen dan de patiënt, behoudens een verplichting daartoe bij of krachtens de wet dan wel een door de patiënt verleende toestemming[4]. Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelovereenkomst en degene die optreedt als vervanger van de hulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden (artikel 7:457 lid 2 BW).

Er is sprake van een onrechtmatige verwerking wanneer gegevens uit het medisch dossier worden ingezien door personen die daartoe niet op grond van artikel 7:457 BW gerechtigd zijn.

---

[1] Kamerstukken II, 1997/98, 25892, nr. 3, p. 98-99.
[2] Artikel 16 Wbp; Kamerstukken II, 1997/98, 25892, nr. 3, p. 22.
[3] De hulpverlener is de natuurlijke persoon of de rechtspersoon waarmee de patiënt een behandelingsovereenkomst heeft afgesloten. De hulpverlener verbindt zich met deze overeenkomst tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op (in dit geval) de patiënt (zie artikel 7: 446 BW).
[4] Ook zonder wettelijke verplichting of toestemming van de patiënt kan de arts zijn zwijgplicht doorbreken. Dit kan zich voordoen indien door het handhaven van die plicht de arts in een noodtoestand in de zin van conflict van plichten zou komen te verkeren. Zie H.J.J. Leenen, J.K.M. Gevers, J. Legemaate, *Handboek gezondheidsrecht, Deel I, Rechten van de mensen in de gezondheidszorg*, Den Haag 2011, p.239.

Maatregelen

De verantwoordelijke zal op grond van artikel 13 Wbp maatregelen moeten treffen om te voorkomen dat andere personen dan die daartoe op grond van artikel 7:457 BW gerechtigd zijn, toegang hebben tot het medisch dossier van betrokkenen. Gezien de aard van de gegevens en de toepasselijkheid van de bijzondere geheimhoudingsplicht van artikel 7:457 BW is daarbij het hoogste beveiligingsniveau vereist.[5]

2. Voorlopige bevindingen

Algemeen

Uit het Handelsregister blijkt dat Dienstapotheek Nijmegen één van de handelsnamen alsmede de vestiging is van Farmazorg BV te Nijmegen. Hieruit blijkt dat Farmazorg BV het doel en de middelen voor de verwerkingen binnen Dienstapotheek Nijmegen vaststelt en derhalve daarvoor de verantwoordelijke is in de zin van de Wbp. Farmazorg BV dient dus passende maatregelen te treffen tegen onbevoegde kennisneming.

De Dienstapotheek Nijmegen verzorgt de avond-, nacht- en weekenddiensten voor de openbare apotheken in Nijmegen en omstreken. Bij de apotheek is het Apotheek Informatie systeem (AIS) Mira in gebruik. In dit systeem worden voor iedere patiënt de geleverde geneesmiddelen vastgelegd. Tevens wordt het systeem gebruikt als ondersteuning bij de medicatiebewaking. De Dienstapotheek heeft geen eigen patiënten.

[5] *Richtsnoeren beveiliging van persoonsgegevens*, College bescherming persoonsgegevens, februari 2013, p. 20 (Stcrt. 2013, 5174) . Deze Richtsnoeren vervangen per 1 maart 2013 de eerdere publicatie G.W. van Blarkom, J.J. Borking, *Beveiliging van persoonsgegevens*, Den Haag: Registratiekamer, Achtergrondstudies en Verkenningen 23, 2001. 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.

Het AIS van Dienstapotheek Nijmegen is aangesloten op de regionale (OZIS-)gegevensuitwisseling van de Stichting OZIS Rijk van Nijmegen (verder te noemen: de stichting). De stichting onderhoudt een zogenaamde centrale patiënten index (CPI) waarin de patiënt is gekoppeld aan diens apotheek van inschrijving. Bij dienstwaarneming vraagt de waarnemend apotheker toestemming aan de patiënt voor raadpleging van de CPI. Vervolgens wordt via een directe lijn (E-zorg) tussen de Dienstapotheek en de apotheek van inschrijving het dossier geraadpleegd.
Deze uitwisseling is geïntegreerd in het AIS.

De door de Dienstapotheek te nemen beveiligingsmaatregelen hebben dus eveneens betrekking op de patiëntgegevens die online, via E-zorg, kunnen worden opgevraagd bij andere apothekers.

Met betrekking tot toegangsbeveiliging en logging zijn, rekening houdend met de stand van de techniek, de kosten van tenuitvoerlegging, de aard van de te beveiligen persoonsgegevens en de toepasselijkheid van artikel 7:457 BW, (onder meer) de onderstaande maatregelen passend - en dus vereist.

Bij de bepaling van hetgeen in de situatie van de apotheek als 'passend beveiligingsniveau' en als 'passende technische en organisatorische maatregelen' in de zin van artikel 13 Wbp moet worden beschouwd zijn de NEN 7510 en -7512 normen als meetinstrument gebruikt. Deze NEN-normen vormen een gezaghebbende sectorale uitwerking van artikel 13 Wbp; de in deze normen beschreven maatregelen worden door partijen uit het veld als adequaat gezien[6], 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.[7]

[6] De status van deze normen wordt ontleend aan de collectiviteit van organisaties uit de zorgsector die betrokken zijn geweest bij het opstellen ervan.
[7] *Richtsnoeren beveiliging van persoonsgegevens*, College bescherming persoonsgegevens, februari 2013.

Toegangsbeveiliging

De NEN 7510 stelt de volgende eis:
"Informatiesystemen, die patiëntgegevens verwerken, behoren authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken."[8]. Daarbij wordt eveneens verwezen naar NEN 7512.[9] Ook uit NEN 7512 (2005) kan worden afgeleid dat twee-factor authenticatie (bijvoorbeeld een chipcard in combinatie met een pincode) in dit geval een vereiste is.[10] Dit vereiste vloeit eveneens voort uit de meer algemene eis dat, in verband met de toepasselijkheid van de bijzondere geheimhoudingsplicht van artikel 7:457 BW, het hoogste beveiligingsniveau moet worden gerealiseerd.[11]

Om in te loggen wordt bij de Dienstapotheek gebruik gemaakt van wachtwoorden. Authenticatie door middel van een wachtwoord is één-factor authenticatie. Daarmee wordt dus niet aan het vereiste van twee-factor authenticatie voldaan, waardoor op dit punt sprake is van overtreding van artikel 13 Wbp.

Logging

Inzake logging is geen overtreding geconstateerd.

[8] NEN 7510 (2011), p. 98.
[9] NEN 7510 (2011), p. 99.
[10] NEN 7512 (2005), p. 7, 11-12 en 15.
[11] Zie hiervoor onder Wettelijk kader - maatregelen.

3. Conclusies voorlopige bevindingen

Het Apothekers Informatiesysteem (AIS) van Dienstapotheek Nijmegen geeft toegang tot zowel de eigen gegevens als de patiëntgegevens bij andere apothekers die zijn aangesloten op de regionale (OZIS-)gegevensuitwisseling van de Stichting OZIS Rijk van Nijmegen.
Om in te loggen in het AIS wordt geen gebruik gemaakt van twee-factor authenticatie maar uitsluitend van een wachtwoord. Farmazorg BV handelt ten aanzien van deze vaststelling in strijd met artikel 13 Wbp.

4. Schriftelijke zienswijze Farmazorg BV

(1) Niemand anders dan de personeelsleden heeft (fysiek) toegang tot de apotheek tenzij onder begeleiding van een personeelslid.

(2) Elk personeelslid heeft een persoonlijke pas om (fysiek) toegang te verkrijgen tot de apotheek.

(3) Alle computers worden na de dienst uitgeschakeld.

(4) Alle computers zijn beveiligd tegen ongeoorloofd opstarten middels een Microsoft username en wachtwoord.

(5) Alle medewerkers hebben hun eigen gebruikersnaam en hun eigen wachtwoord binnen het AIS MIRA.

(6) De apotheek heeft voor alle medewerkers een UZI-pas aangevraagd, waardoor twee-factor authenticatie per heden een feit is.

5. Reactie CBP

(1) (2) (3) Deze opmerkingen hebben betrekking op de *fysieke* toegangsbeveiliging. Twee-factor authenticatie, zoals bedoeld in de bevindingen van het CBP, vormt onderdeel van de zogeheten *logische* toegangsbeveiliging. Dat is toegangsbeveiliging die geprogrammeerd is in (systeem-)software, zoals vragen om een gebruikersnaam en wachtwoord. De opmerking heeft dus geen betrekking op de door het CBP geconstateerde overtreding.

(4) Dat medewerkers van de apotheek ook voor het besturingssysteem (Microsoft Windows) een wachtwoord moeten intoetsen, maakt niet dat hierdoor sprake is van twee-factor authenticatie. Daarvoor is nodig dat een *andere* authenticatiefactor wordt toegepast. Twee-factor authenticatie vereist namelijk de inzet van twee van de volgende factoren: kennis (bijvoorbeeld een wachtwoord of pincode), bezit (bijvoorbeeld een pasje) en zogeheten inherentie (d.w.z. een relatie met de fysieke of anderszins onlosmakelijke eigenschappen van de systeemgebruiker, zoals een vingerafdruk of irisscan).
Het meerdere malen vragen van een wachtwoord vormt dus geen twee-factor authenticatie.

(5) Een gebruikersnaam dient ter *identificatie* (welke medewerker wil toegang tot het systeem?). Vervolgens is (bijvoorbeeld) een wachtwoord nodig voor de *authenticatie* (is de medewerker daadwerkelijk wie hij/zij zegt te zijn?). Dat medewerkers om toegang tot het AIS te krijgen hun persoonlijke gebruikersnaam en wachtwoord moeten intoetsen, vormt dus niet de vereiste twee-factor authenticatie. Er is hier namelijk sprake van maar één factor: het wachtwoord (zie verder punt 4).

(6) Met een UZI-pas (met pincode) kan inderdaad twee-factor authenticatie tot stand worden gebracht. Er is dan namelijk sprake van twee afzonderlijke

authenticatiemiddelen: iets wat je hebt (UZI-pas) en iets wat je weet (pincode). Maar voordat het CBP kan aannemen dat twee-factor authenticatie daadwerkelijk een feit is bij de Dienstapotheek, moet deze eerst aantonen dat het AIS zo is aangepast en/of ingericht dat medewerkers zonder UZI-pas niet (meer) kunnen inloggen. Het feit dat de Dienstapotheek UZI-passen voor alle medewerkers heeft aangevraagd, zegt dus nog niets over de praktijk.

De schriftelijke zienswijze van de Dienstapotheek Nijmegen geeft het CBP aldus geen reden om de bevindingen aan te passen. Het CBP acht vooralsnog niet aangetoond dat de geconstateerde overtreding inmiddels is beëindigd.

6. Definitieve conclusies

Het Apothekers Informatiesysteem (AIS) van Dienstapotheek Nijmegen geeft toegang tot zowel de eigen gegevens als de patiëntgegevens bij andere apothekers die zijn aangesloten op de regionale (OZIS-)gegevensuitwisseling van de Stichting OZIS Rijk van Nijmegen.
Om in te loggen in het AIS wordt geen gebruik gemaakt van twee-factor authenticatie maar uitsluitend van een wachtwoord. Farmazorg BV handelt ten aanzien van deze vaststelling in strijd met artikel 13 Wbp.

Naar aanleiding van de voorlopige bevindingen heeft Farmazorg BV maatregelen getroffen om de geconstateerde overtreding van artikel 13 Wbp te beëindigen. Het CBP concludeert evenwel dat vooralsnog niet is aangetoond dat deze maatregelen afdoende zijn.

Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College