COLLEGE BESCHERMING PERSOONSGEGEVENS

College bescherming persoonsgegevens

Onderzoek naar de verwerking van medicatiegegevens door Apotheek De Witte Pauw BV te Ermelo

Z2013-127

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 Nijmegen en tussen twee apotheken in Ermelo, waaronder Apotheek De Witte Pauw.

Apotheek De Witte Pauw BV is verantwoordelijke in de zin van de Wbp voor de gegevensverwerkingen bij Apotheek De Witte Pauw 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.

Apotheek De Witte Pauw is lid van de Vereniging van apothekers betrokken bij de dienstwaarnemingspost Harderwijk. Met behulp van de door deze vereniging beheerde Centrale Patiëntenindex (CPI) kan Apotheek De Witte Pauw patiëntgegevens inzien van andere apothekers in de regio Harderwijk (en vice versa). Hierdoor wordt het aantal patiënten waarvan gegevens kunnen worden ingezien aanzienlijk vergroot.

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.

Uit NEN 7512 volgt dat maatregelen moeten worden getroffen om te voorkomen dat wachtwoorden bij anderen bekend worden. Op het

inlogscherm van het Apothekers Informatiesysteem (AIS) is het ingetypte wachtwoord zichtbaar.

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

Apotheek De Witte Pauw BV heeft niet aannemelijk gemaakt dat dat de geplande nieuwe versie van Pharmacom een einde maakt aan deze bij Apotheek De Witte Pauw BV geconstateerde overtredingen.

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 Apotheek De Witte Pauw (hierna ook wel: de apotheek). Apotheek De Witte Pauw is lid van de Vereniging van apothekers betrokken bij de dienstwaarnemingspost Harderwijk. Met behulp van de door deze vereniging beheerde Centrale Patiëntenindex (CPI) kan Apotheek De Witte Pauw patiëntgegevens inzien van andere apothekers in de regio Harderwijk (en vice versa). Hierdoor wordt het aantal patiënten waarvan gegevens kunnen worden ingezien aanzienlijk vergroot. Dit maakt dat toegangscontrole en logging niet alleen betrekking hebben op de gegevens van de patiënten van Apotheek De Witte Pauw, maar ook op die van deze andere apotheken.

Op 25 februari 2013 heeft het CBP een interview gehouden met de directeur, tevens beherend apotheker van Apotheek De Witte Pauw. Ook werd door haar een demonstratie gegeven van de voor dit onderzoek relevante onderdelen van de gebruikte systemen. Tijdens dit onderzoek is schriftelijk bewijsmateriaal verkregen.

Eerder werden op 21 november 2012 interviews gehouden met de voorzitter en de OZIS-beheerder van de Vereniging van apothekers betrokken bij de dienstwaarnemingspost Harderwijk.

Bij brief van 22 juli 2013 is het rapport voorlopige bevindingen naar De Witte Pauw BV verzonden. De Witte Pauw BV heeft op 5 september 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 Apotheek De Witte Pauw de (enige) vestiging is van Apotheek De Witte Pauw BV te Ermelo. Hieruit blijkt dat Apotheek De Witte Pauw BV het doel en de middelen voor de verwerkingen binnen Apotheek De Witte Pauw vaststelt en derhalve daarvoor de verantwoordelijke is in de zin van de Wbp. Apotheek De Witte Pauw BV dient dus passende maatregelen te treffen tegen onbevoegde kennisneming.

Bij de apotheek is het Apotheek Informatie systeem (AIS) Pharmacom in gebruik. In dit systeem worden voor iedere patiënt de geleverde geneesmiddelen vastgelegd. Tevens wordt het systeem gebruikt als ondersteuning bij de medicatiebewaking.

Daarnaast is het AIS van Apotheek De Witte Pauw aangesloten op de regionale (OZIS-)gegevensuitwisseling van de Vereniging van apothekers betrokken bij de dienstwaarnemingspost Harderwijk (verder te noemen: de vereniging). De vereniging onderhoudt een zogenaamde centrale patiënten index (CPI) waarin naam en bsn van de patiënt zijn gekoppeld aan diens apotheek van inschrijving. Bij dienstwaarneming

[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.

vraagt de waarnemend apotheker toestemming aan de patiënt voor raadpleging van de CPI. Vervolgens wordt via een directe lijn (E-zorg) tussen de waarnemende apotheek en de apotheek van inschrijving het dossier geraadpleegd.

Deze uitwisseling is een geïntegreerde, tweeledige functie in het AIS: enerzijds kunnen vanuit het AIS gegevens van andere apothekers worden geraadpleegd en anderzijds zijn de medicatiegegevens van de eigen patiënten in het AIS beschikbaar voor andere bij de vereniging aangesloten apothekers.

De door de apotheek te nemen beveiligingsmaatregelen hebben dus betrekking op zowel de eigen patiëntgegevens als 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

Identificatie

NEN 7510 vereist het gebruik van unieke gebruikersidentificaties (ID) zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun handelingen.[8]

Om in te loggen wordt bij de apotheek gebruik gemaakt van een groepsaccount.

Hiermee wordt niet voldaan aan het vereiste dat elke gebruiker uniek wordt geïdentificeerd. Deze unieke identificatie is, zoals hierboven aangegeven, één van de passende maatregelen die getroffen moet worden krachtens artikel 13 Wbp. Derhalve is sprake van overtreding van artikel 13 Wbp.

Authenticatie

Wachtwoord of PIN-code moet geheim zijn

Als middel voor authenticatie wordt geheime kennis (wachtwoord of PIN-code) het meest toegepast. Maatregelen moeten worden getroffen om te voorkomen dat dit geheim bij anderen dan de betreffende entiteit bekend wordt.[9]
Om in te loggen wordt bij Apotheek De Witte Pauw gebruik gemaakt van een groepsaccount met (dus ook) gedeelde wachtwoorden. Op het inlogscherm van het Apothekers Informatiesysteem (AIS) is bovendien het ingetypte wachtwoord zichtbaar. Eén en ander is een overtreding van artikel 13 Wbp.

Gebruik van wachtwoord niet voldoende

De NEN 7510 stelt bovendien de volgende eis:
"Informatiesystemen, die patiëntgegevens verwerken, behoren authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken."[10]. Daarbij wordt

[8] NEN 7510 (2011), p. 89.
[9] NEN 7512 (2005), p. 11.
[10] NEN 7510 (2011), p. 98.

eveneens verwezen naar NEN 7512.[11] 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.[12] 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.[13]

Om in te loggen wordt 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 eveneens sprake is van overtreding van artikel 13 Wbp.

Logging

Inzake logging is geen overtreding geconstateerd.

3. Conclusies voorlopige bevindingen

Het Apothekers Informatiesysteem (AIS) van Apotheek De Witte Pauw geeft toegang tot zowel de eigen patiëntgegevens als de patiëntgegevens bij andere apothekers die zijn aangesloten op de regionale (OZIS-)gegevensuitwisseling van de Vereniging van apothekers betrokken bij de dienstwaarnemingspost Harderwijk.
Om in te loggen in het AIS wordt gebruik gemaakt van een groepsaccount met (dus ook) gedeelde wachtwoorden. Op het inlogscherm van het AIS is bovendien het ingetypte wachtwoord zichtbaar. Bij het inloggen wordt geen gebruik gemaakt van twee-factor authenticatie. Apotheek De Witte Pauw BV handelt ten aanzien van deze vaststellingen in strijd met artikel 13 Wbp.

4. Schriftelijke zienswijze De Witte Pauw BV

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

(a) Constatering CBP (1): Om in te loggen in het AIS wordt gebruik gemaakt van een groepsaccount met (dus ook) gedeelde wachtwoorden.

Reactie De Witte Pauw BV:
Dit is niet juist. Het is niet zo dat er groepscodes gebruikt worden. De codes zijn individueel bepaald.

(b) Constatering CBP (2): Op het inlogscherm van het AIS is bovendien het ingetypte wachtwoord zichtbaar.

Reactie De Witte Pauw BV:
Dit is niet juist. Het CBP heeft de (op het scherm zichtbare) tweeletterige AIS-gebruikerscode aangezien voor een wachtwoord.

(c) Constatering CBP (3): Bij het inloggen wordt geen gebruik gemaakt van twee-factor authenticatie.

Reactie De Witte Pauw BV:
Per 1 januari 2014 gaan alle apothekers over naar Pharmacom Nieuw. Hierin zijn de inlogmogelijkheden uitgebreider. Hierin wordt telkens twee keer een inlogcode van 5 à 8 karakters gevraagd.

(d) Algemeen

1. Per 1 januari 2014 gaan alle apothekers over naar Pharmacom Nieuw.
2. Huidige tekortkoming is niet een tekortkoming van Apotheek De Witte Pauw maar een landelijk probleem.

5. Reactie CBP

(a) Het CBP zal de bevindingen corrigeren op het punt van identificatie en deels op het punt van authenticatie. Uit de reactie van Apotheek De Witte Pauw BV is namelijk gebleken dat er geen sprake is van een gezamenlijk account (identificatie) en dus ook niet van gedeelde wachtwoorden (authenticatie). Het CBP past constatering (1) dus aan.

(b) Het CBP blijft echter bij de constatering (2) dat het wachtwoord zichtbaar is (authenticatie). Tijdens de demonstratie hebben alle drie de CBP-medewerkers het wachtwoord op het beeldscherm gezien. Dit betrof niet de tweeletterige AIS-gebruikerscode. Er is er geen aanleiding om aan de juistheid van deze waarneming te twijfelen.

(c) Het twee keer vragen van inlogcodes (wachtwoorden die bestaan uit cijfers), van welke lengte dan ook, vormt geen twee-factor authenticatie. Daarvoor is nodig dat naast een inlogcode 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). Constatering (3) van het CBP, dat er geen sprake is van twee-factor authenticatie, blijft daarom eveneens gehandhaafd.

(d.1) Het staat vooralsnog niet vast dat de nieuwe versie van Pharmacom een einde maakt aan de bij Apotheek De Witte Pauw BV geconstateerde overtredingen (zie punt b: het is nog niet duidelijk of in de nieuwe versie het wachtwoord wél onzichtbaar is, en zie punt c: twee keer vragen om inlogcodes zorgt niet voor de vereiste twee-factor authenticatie) . Apotheek De Witte Pauw BV heeft daarom niet aannemelijk gemaakt dat de geconstateerde overtredingen zijn beëindigd dan wel op redelijke termijn beëindigd zullen worden.

(d.2) Apotheek De Witte Pauw BV is verantwoordelijke in de zin van de Wet bescherming persoonsgegevens voor zijn gegevensverwerkingen. Eventuele landelijke problematiek doet hier niets aan af. De apotheek blijft zelf verantwoordelijk voor adequate beveiliging van medische gegevens.

6. Definitieve conclusies

Het Apothekers Informatiesysteem (AIS) van Apotheek De Witte Pauw geeft toegang tot zowel de eigen patiëntgegevens als de patiëntgegevens bij andere apothekers die zijn aangesloten op de regionale (OZIS-)gegevensuitwisseling van de Vereniging van apothekers betrokken bij de dienstwaarnemingspost Harderwijk.
Op het inlogscherm van het AIS is het ingetypte wachtwoord zichtbaar. Bij het inloggen wordt geen gebruik gemaakt van twee-factor authenticatie. Apotheek De Witte Pauw BV handelt ten aanzien van deze vaststellingen in strijd met artikel 13 Wbp.

Apotheek De Witte Pauw BV heeft niet aannemelijk gemaakt dat dat de geplande nieuwe versie van Pharmacom een einde maakt aan deze bij Apotheek De Witte Pauw BV geconstateerde overtredingen.

Het College bescherming persoonsgegevens,
Voor het College,

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