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

College bescherming persoonsgegevens

Onderzoek naar het gebruik van waarneemdossiers bij Stichting Gezondheidscentra Haarlemmermeer

z2012-00623

Rapport definitieve bevindingen

21 augustus 2013

SAMENVATTING

Het College bescherming persoonsgegevens (CBP) heeft in 2012-2013 onderzoek gedaan naar toegangsbeveiliging en logging bij het gebruik van waarneemdossiers door Stichting Gezondheidscentra Haarlemmermeer te Hoofddorp.

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

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.

NEN 7510 vereist het gebruik van unieke gebruikersidentificaties (ID) zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun handelingen. Waarnemers op de huisartsenpost loggen echter in onder de naam van de huisarts voor wie ze werken.

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

Alle raadplegingen van het medisch dossier moeten worden gelogd. Deze logging dient regelmatig te worden gecontroleerd op onbevoegde raadplegingen. Bij de huisartsenpost Haarlemmermeer worden de logbestanden niet regelmatig gecontroleerd op onbevoegde raadplegingen en hiervoor ontbreken procedures.

Naar aanleiding van de voorlopige bevindingen heeft Stichting Gezondheidscentra Haarlemmermeer diverse maatregelen op de korte en lange(re) termijn getroffen om de geconstateerde overtredingen van artikel 13 Wbp te beëindigen.

Het CBP concludeert dat - voor zover thans bekend - de geconstateerde overtredingen op dit moment nog voortduren maar naar verwachting in september 2013 zullen zijn beëindigd.

1. Inleiding

Het College bescherming persoonsgegevens (CBP) heeft in 2012-2013 onderzoek gedaan naar toegangsbeveiliging en logging bij het gebruik van waarneemdossiers[1] door drie huisartsenposten (met ieder een ander systeem voor gegevensuitwisseling).

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 waarneemdossier wordt gebruikt door huisartsenposten waar patiënten worden geholpen op momenten dat zij niet bij hun eigen huisarts terecht kunnen.

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

Eén van de onderzochte huisartsenposten is de huisartsenpost Haarlemmermeer. De Stichting Gezondheidscentra Haarlemmermeer verzorgt hier de nacht-, avond- en weekendzorg voor patiënten van deelnemende huisartsen in Haarlemmermeer. Op 10 oktober 2012 heeft het CBP interviews gehouden met de directeur, de locatiemanager, de systeembeheerder, een deelnemende huisarts en een huisartsassistente. Ook werd door de medewerkers van de huisartsenpost een demonstratie gegeven van de voor dit onderzoek relevante onderdelen van de gebruikte systemen. Tijdens dit onderzoek is schriftelijk bewijsmateriaal verkregen.

[1] Het waarneemdossier wordt ook wel professionele samenvatting genoemd. Deze samenvatting bevat administratieve gegevens zoals naam, geboortedatum, adres van de patiënt en de naam van diens huisarts. Daarnaast bevat de professionele samenvatting relevante gegevens over de gezondheid: medicatie, allergieën, contra-indicaties en de recente belangrijkste aandoeningen (episoden). De beroepsgroep zelf heeft vastgesteld welke informatie in geval van waarneming relevant is. In dit onderzoek zijn ook eventuele andere in het kader van de waarneming uitgewisselde gegevens betrokken.

Bij brief van 17 juni 2013 is het rapport voorlopige bevindingen naar Stichting Gezondheidscentra Haarlemmermeer verzonden. Stichting Gezondheidscentra Haarlemmermeer heeft op 27 juni 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.[2] Gegevens betreffende de gezondheid worden aangemerkt als bijzondere ofwel gevoelige gegevens.[3]

Onrechtmatige verwerking

In artikel 7:457, lid 1, van het Burgerlijk Wetboek (BW) is bepaald dat de hulpverlener[4] 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.[5] 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.

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

---

[2] Kamerstukken II, 1997/98, 25892, nr. 3, p. 98-99.

[3] Artikel 16 Wbp; Kamerstukken II, 1997/98, 25892, nr. 3, p. 22.

[4] 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).

[5] 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.

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.[6]

2. Voorlopige bevindingen

Algemeen

Uit het Handelsregister, uit de informatie op de website www.gezondheidscentrahaarlemmermeer.nl en uit de interviews blijkt dat Stichting Gezondheidscentra Haarlemmermeer het doel en de middelen voor de verwerkingen binnen de huisartsenpost Haarlemmermeer vaststelt en derhalve daarvoor de verantwoordelijke is in de zin van de Wbp. Stichting Gezondheidscentra Haarlemmermeer dient dus passende maatregelen te treffen tegen onbevoegde kennisneming.

Bij de huisartsenpost is onder andere het volgende systeem in gebruik:

-[…]: dit is het patiëntinformatie- en workflowsysteem van de huisartsenpost, waarin de afspraken met de patiënten worden geagendeerd, eventueel waarneemdossiers kunnen worden geraadpleegd, gegevens kunnen worden vastgelegd tijdens een consult etc.

In dit systeem worden medische gegevens verwerkt waarop de bijzondere geheimhoudingsplicht van artikel 7:457 BW rust.

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

[6] *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.

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 huisartsenpost als 'passend beveiligingsniveau' en als 'passende technische en organisatorische maatregelen' in de zin van artikel 13 Wbp moet worden beschouwd zijn de NEN-normen 7510-7513 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[7], 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.[8]

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.[9]

Zogenaamde waarnemers[10] op de huisartsenpost loggen in onder de naam van de huisarts voor wie ze werken.

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.

---

[7] De status van deze normen wordt ontleend aan de collectiviteit van organisaties uit de zorgsector die betrokken zijn geweest bij het opstellen ervan.
[8] *Richtsnoeren beveiliging van persoonsgegevens*, College bescherming persoonsgegevens, februari 2013.
[9] NEN 7510 (2011), p. 89.
[10] Dit zijn ingehuurde freelance huisartsen die invallen/waarnemen voor de aan de huisartsenpost deelnemende huisartsen.

Authenticatie

De NEN 7510 stelt de volgende eis:

"Informatiesystemen, die patiëntgegevens verwerken, behoren authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken."[11]. Daarbij wordt eveneens verwezen naar NEN 7512.[12] 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.[13] 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.[14]

Artsen en assistenten op de huisartsenpost loggen in op het systeem [...] met een gebruikersnaam en een wachtwoord. Authenticatie door middel van een wachtwoord is één-factor authenticatie. Voor deze systemen wordt dus niet aan het vereiste van twee-factor authenticatie voldaan, waardoor op dit punt sprake is van overtreding van artikel 13 Wbp.

Logging

Volgens de NEN-normen 7510 en 7513 moeten de raadplegingen van het medisch dossier worden gelogd.[15] Deze logging dient regelmatig te worden gecontroleerd op onbevoegde raadplegingen.[16] [17] Uit het onderzoek blijkt dat incidenten (onrechtmatige inzage) uiteindelijk traceerbaar zijn in [systeem]. De logbestanden worden echter niet regelmatig gecontroleerd op onbevoegde raadplegingen en hiervoor ontbreken procedures. De Stichting Gezondheidscentra Haarlemmermeer handelt op dit punt niet in overeenstemming met artikel 13 Wbp.

---

[11] NEN 7510 (2011), p. 98.
[12] NEN 7510 (2011), p. 99.
[13] NEN 7512 (2005), p. 7, 11-12 en 15.
[14] Zie hiervoor onder Wettelijk kader - maatregelen.
[15] NEN 7510 (2011), p. 83, 87, 88; NEN 7513, p. 14.
[16] NEN 7510 (2011), p. 83.
[17] Zie tevens EHRM 17 juli 2008, nr. 20511/03, RvdW 2009, 295.

3. Conclusies voorlopige bevindingen

Waarnemers op de huisartsenpost loggen in onder de naam van de huisarts voor wie ze werken.
Bij het inloggen op het systeem [...] wordt geen gebruik gemaakt van twee-factor authenticatie maar uitsluitend van een wachtwoord.
De logbestanden worden niet regelmatig gecontroleerd op onbevoegde raadplegingen en hiervoor ontbreken procedures.

Stichting Gezondheidscentra Haarlemmermeer handelt ten aanzien van deze vaststellingen in strijd met artikel 13 Wbp.

4. Schriftelijke zienswijze Stichting Gezondheidscentra Haarlemmermeer

Constatering CBP (1): Waarnemers op de huisartsenpost loggen in onder de naam van de huisarts voor wie ze werken.

Reactie Stichting Gezondheidscentra Haarlemmermeer:
(1) Het gebruikte systeem ([...]) staat op dit moment geen gastgebruik toe. Dit probleem zal worden verholpen in een nieuwe release die in augustus 2013 zal worden geïnstalleerd.
(2) Tot dat moment zet de waarnemer bij elk patiëntcontact zijn naam in het dossier.

Constatering CBP (2): Op de huisartsenpost wordt uitsluitend gebruik gemaakt van wachtwoorden.

Reactie Stichting Gezondheidscentra Haarlemmermeer:
Zodra gastgebruik mogelijk is (zie hierboven) zal het gebruik van de UZI-pas algemeen worden ingevoerd.

Constatering CBP (3): Bij de huisartsenpost Haarlemmermeer worden de logbestanden niet regelmatig gecontroleerd op onbevoegde raadplegingen en hiervoor ontbreken procedures.

Reactie Stichting Gezondheidscentra Haarlemmermeer:
Hiervoor wordt een procedure opgesteld die in augustus 2013 zal worden ingevoerd.

5. Reactie CBP

Maatregel (2) met betrekking tot Constatering CBP (1) - het door de waarnemer vermelden van zijn naam in het dossier - acht het CBP op zichzelf onvoldoende om te voldoen aan de eis dat elke gebruiker uniek wordt geïdentificeerd. Zo'n vermelding kan immers worden vergeten en leidt niet zonder meer tot een waterdichte koppeling tussen de gebruiker en zijn systeemhandelingen.

De constateringen en conclusies in de voorlopige bevindingen worden overigens niet bestreden, waardoor de bevindingen geen aanpassing behoeven. Wel acht het CBP het op grond van de schriftelijke zienswijze van de Stichting Gezondheidscentra Haarlemmermeer aannemelijk dat de geconstateerde overtredingen op redelijke termijn beëindigd zullen worden.[18]

6. Definitieve conclusies

Waarnemers op de huisartsenpost loggen in onder de naam van de huisarts voor wie ze werken. Bij het inloggen op het systeem [...] wordt geen gebruik gemaakt van twee-factor authenticatie maar uitsluitend van een wachtwoord. De logbestanden worden niet regelmatig gecontroleerd op onbevoegde raadplegingen en hiervoor ontbreken procedures. Stichting Gezondheidscentra Haarlemmermeer handelt ten aanzien van deze vaststellingen in strijd met artikel 13 Wbp.

[18] Met de invoering van de UZI-pas zal sprake zijn van twee-factor authenticatie: iets dat je hebt (UZI-pas) en iets dat je weet (PIN-code).

Naar aanleiding van de voorlopige bevindingen heeft Stichting Gezondheidscentra Haarlemmermeer diverse maatregelen op de korte en lange(re) termijn getroffen om de geconstateerde overtredingen van artikel 13 Wbp te beëindigen.

Het CBP concludeert dat - voor zover thans bekend - de geconstateerde overtredingen op dit moment nog voortduren maar naar verwachting in september 2013 zullen zijn beëindigd.

Het College bescherming persoonsgegevens,
Voor het College,

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