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 Centrale Huisartsenpost Nightcare BV te Heerlen

z2012-00624

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 Centrale Huisartsenpost Nightcare BV te Heerlen.

Centrale Huisartsenpost Nightcare BV is verantwoordelijke in de zin van de Wbp voor de gegevensverwerkingen bij de huisartsenpost Heerlen 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, authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken (twee-factor authenticatie).
Op de huisartsenpost werd ten tijde van het onderzoek echter uitsluitend gebruik gemaakt van wachtwoorden. Naar aanleiding van de voorlopige bevindingen heeft Centrale Huisartsenpost Nightcare BV maatregelen op de korte en lange(re) termijn getroffen om deze overtreding van artikel 13 Wbp te beëindigen. Het CBP concludeert dat deze overtreding op dit moment nog voortduurt maar naar verwachting eind 2013 zal zijn beëindigd.

Op de huisartsenpost werden ten tijde van het onderzoek zogenaamde viewers gebruikt waarmee patiëntgegevens kunnen worden ingezien bij andere zorgaanbieders. Het opvragen van patiëntgegevens via deze viewers

zou vanwege artikel 13 Wbp (technisch) moeten worden beperkt tot patiënten, die op dat moment bij de huisartsenpost in behandeling zijn. Dit was niet het geval. Naar aanleiding van de voorlopige bevindingen heeft Centrale Huisartsenpost Nightcare BV afdoende maatregelen getroffen om deze overtreding van artikel 13 Wbp te beëindigen. Het CBP concludeert dat deze overtreding thans is 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 Heerlen. Centrale Huisartsenpost Nightcare BV verzorgt hier de nacht-, avond- en weekendzorg voor patiënten van deelnemende huisartsen in Heerlen en omstreken.

Op 6 november 2012 heeft het CBP interviews gehouden met de directeur, de locatiemanager en een deelnemende huisarts. Ook werd door de medewerkers van de huisartsenpost een demonstratie gegeven van de voor dit onderzoek relevante onderdelen van de gebruikte systemen. Op 19 februari 2013 heeft het CBP nogmaals

[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.

interviews gehouden met de locatiemanager en de hiervoor bedoelde huisarts. Tijdens deze onderzoeken is schriftelijk bewijsmateriaal verkregen.

Bij brief van 17 juni 2013 is het rapport voorlopige bevindingen naar Centrale Huisartsenpost Nightcare BV verzonden. Centrale Huisartsenpost Nightcare BV 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 gerechtigd zijn, toegang hebben tot het medisch dossier van betrokkenen. Gezien de

---

[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.

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.nightcare-ozl.nl en uit de interviews blijkt dat Centrale Huisartsenpost Nightcare BV het doel en de middelen voor de verwerkingen binnen de huisartsenpost Heerlen vaststelt en derhalve daarvoor de verantwoordelijke is in de zin van de Wbp. Centrale Huisartsenpost Nightcare BV dient dus passende maatregelen te treffen tegen onbevoegde kennisneming.

Bij de huisartsenpost zijn, zo blijkt uit het onderzoek, onder andere de volgende systemen in gebruik:

- [A]: 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.;
- [B]: dit is een zogenaamde viewer waarmee in de via de regionale OZIS-ring[7] beschikbare medicatiegegevens kan worden gekeken;
- [C]: Dit is een zogenaamde viewer waarmee in (een deel van de) patiëntgegevens van [zorginstelling] kan worden gekeken.

De systemen [B] en [C] worden alleen gebruikt door medewerkers met een coördinerende functie (regie-arts en Eerst Verantwoordelijke Assistente (EVA)).

---

[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.

[7] Dit is een regionaal netwerk waarop elektronische uitwisseling van gegevens tussen apotheken en huisartsen plaats vindt volgens de zogenaamde (landelijke) OZIS-standaard.

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

Toegangsbeveiliging

Met betrekking tot de toegangsbeveiliging 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 huisartsenpost 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[8], 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.[9]

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."[10]. Daarbij wordt 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

---

[8] De status van deze normen wordt ontleend aan de collectiviteit van organisaties uit de zorgsector die betrokken zijn geweest bij het opstellen ervan.

[9] Richtsnoeren *beveiliging van persoonsgegevens*, College bescherming persoonsgegevens, februari 2013.

[10] NEN 7510 (2011), p. 98.

[11] NEN 7510 (2011), p. 99.

[12] NEN 7512 (2005), p. 7, 11-12 en 15.

toepasselijkheid van de bijzondere geheimhoudingsplicht van artikel 7:457 BW, het hoogste beveiligingsniveau moet worden gerealiseerd.[13]

Artsen en assistenten op de huisartsenpost loggen in op het systeem [A] met een gebruikersnaam en een wachtwoord. Regie-arts en EVA loggen in op het systeem [B] met een gebruikersnaam en 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.

Toets op behandelrelatie
Uit het wettelijk kader (zie hiervoor onder "Wettelijk kader") vloeit voort dat, wanneer in het kader van dienstwaarneming toegang wordt gezocht tot gegevens die behoren tot het medisch dossier van een patiënt, het door de verantwoordelijke gebruikte systeem zo mogelijk dient te controleren of degene die toegang zoekt op dat moment de hulpverlener van de betrokkene of diens vervanger is, dan wel rechtstreeks bij de uitvoering van de behandelingsovereenkomst is betrokken. Indien dit het geval is kan toegang tot de persoonsgegevens worden verleend. Anders dient toegang te worden geweigerd.

In het systeem [B] hebben de regie-arts en EVA na inloggen toegang tot de medicatiegegevens van *alle* patiënten in de OZIS-regio. In het systeem [C] hebben regie-arts en EVA na inloggen toegang tot (medische) gegevens van *alle* patiënten in [zorginstelling]. Deze systemen bieden een (veel) te ruime toegang tot de beschikbare patiëntgegevens, waardoor op dit punt sprake is van overtreding van artikel 13 Wbp juncto artikel 7:457 BW. Het opvragen van patiëntgegevens via deze systemen zou (technisch) moeten worden beperkt tot patiënten, die op dat moment bij de huisartsenpost in behandeling zijn.

Logging

Inzake logging is geen overtreding geconstateerd.

[13] Zie hiervoor onder Wettelijk kader - maatregelen.

3. Conclusies voorlopige bevindingen

Bij het inloggen op de systemen [A] en [B] wordt geen gebruik gemaakt van twee-factor authenticatie maar uitsluitend van een wachtwoord. De systemen [B] en [C] bieden daarnaast een te ruime toegang tot de (extern) beschikbare patiëntgegevens. Centrale Huisartsenpost Nightcare BV handelt ten aanzien van beide vaststellingen in strijd met artikel 13 Wbp.

4. Schriftelijke zienswijze Centrale Huisartsenpost Nightcare BV

Constatering CBP (1): In het systeem [C] hebben regie-arts en EVA na inloggen toegang tot (medische) gegevens van alle patiënten in [zorginstelling].

Reactie Centrale Huisartsenpost Nightcare BV: Dit is feitelijk onjuist. Alleen artsen, en niet EVA, hebben toegang tot [C].

Constatering CBP (2): Op de huisartsenpost wordt uitsluitend gebruik gemaakt van wachtwoorden (dit betreft de systemen [A] en [B]).

Reactie Centrale Huisartsenpost Nightcare BV: [B] is inmiddels gedeactiveerd, dus niet meer toegankelijk.
De huisartsenpost zal de UZI-pas nog dit jaar implementeren. De technische infrastructuur is hiervoor reeds geschikt en voor al het (medisch) personeel op de huisartsenpost zijn UZI-passen aangevraagd.

Constatering CBP (3): Op de huisartsenpost worden zogenaamde viewers ([C] en [B]) gebruikt waarmee patiëntgegevens kunnen worden ingezien bij andere zorgaanbieders.

Reactie Centrale Huisartsenpost Nightcare BV: Technisch is deze toegang niet te beperken. De viewers zijn inmiddels gedeactiveerd.

5. Reactie CBP

De voorlopige bevindingen dienen te worden gecorrigeerd naar aanleiding van hetgeen Centrale Huisartsenpost Nightcare BV heeft opgemerkt ten aanzien van de toegang van EVA tot [C] (constatering CBP (1)).

Overigens worden de constateringen en conclusies in de voorlopige bevindingen niet bestreden, waardoor de bevindingen verder geen aanpassing behoeven. Wel acht het CBP het, op grond van de schriftelijke zienswijze van Centrale Huisartsenpost Nightcare BV, aannemelijk dat de overtredingen deels zijn beëindigd en overigens op redelijke termijn beëindigd zullen worden.[14]

6. Definitieve conclusies

Het CBP stelt vast dat ten tijde van het onderzoek (a) bij het inloggen op de systemen [A] en [B] geen gebruik werd gemaakt van twee-factor authenticatie maar uitsluitend van een wachtwoord en (b) de systemen [B] en [C] daarnaast een te ruime toegang boden tot de (extern) beschikbare patiëntgegevens. Centrale Huisartsenpost Nightcare BV handelde ten aanzien van beide vaststellingen in strijd met artikel 13 Wbp.

Naar aanleiding van de voorlopige bevindingen heeft Centrale Huisartsenpost Nightcare BV diverse maatregelen op de korte en lange(re) termijn getroffen om de geconstateerde overtredingen van artikel 13 Wbp te beëindigen.

Het CBP concludeert dat overtreding (a) voor wat betreft het systeem [B] en overtreding (b) op dit moment zijn beëindigd. Het CBP concludeert dat overtreding (a) voor wat betreft het systeem [A] op dit moment nog voortduurt maar naar verwachting eind 2013 zal zijn beëindigd.

[14] 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).

Hoogachtend,

Het College bescherming persoonsgegevens,
Voor het College,

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