

College bescherming persoonsgegevens

Onderzoek naar het gebruik van waarneemdossiers bij Coöperatieve
Huisartsendienst Twente-Oost U.A.

z2012-00622

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 Coöperatieve Huisartsdienst Twente-Oost U.A.

Coöperatieve Huisartsdienst Twente-Oost U.A. is verantwoordelijke in de zin van de Wbp voor de gegevensverwerkingen bij de huisartsenpost Enschede 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.

Artikel 13 Wbp, zoals nader ingevuld door de richtsnoeren van het CBP en de NEN 7510 norm, vereist het gebruik van unieke gebruikersidentificaties (ID) zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun handelingen.

Met een niet op naam gestelde UZI-leenpas konden ten tijde van het onderzoek patiëntgegevens worden opgevraagd uit het huisartsinformatiesysteem (HIS) van een bij de huisartsenpost Enschede aangesloten huisarts. Hiermee werd niet voldaan aan het vereiste dat elke gebruiker uniek wordt geïdentificeerd. Het CBP concludeert dat deze overtreding van artikel 13 Wbp thans is beëindigd.

1. Inleiding

Het College bescherming persoonsgegevens (CBP) heeft in 2012-2013 onderzoek gedaan naar toegangsbeveiliging en logging bij het gebruik van waarneemdossiers¹ 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 Enschede. Coöperatieve Huisartsendienst Twente-Oost U.A. (verder te noemen: HDT-Oost) verzorgt hier de nacht-, avond- en weekendzorg voor patiënten van deelnemende huisartsen in de gemeenten Enschede en Haaksbergen. Op 31 oktober 2012 heeft het CBP interviews gehouden met de directeur, een (externe) ICT-deskundige van leverancierszijde 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.

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 HDT-Oost verzonden. HDT-Oost heeft op 24 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 hulpverlener⁴ 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 en uit de interviews blijkt dat HDT-Oost het doel en de middelen voor de verwerkingen binnen de huisartsenpost Enschede vaststelt en derhalve daarvoor de verantwoordelijke is in de zin van de Wbp. HDT-Oost dient dus passende maatregelen te treffen tegen onbevoegde kennisneming.

Bij de huisartsenpost Enschede is het systeem [...] in gebruik. Dit is het patiëntinformatie- en workflowsysteem van de huisartsenpost, waarin de afspraken met de patiënten worden geagendeerd, 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.

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.

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.

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 is de NEN 7510 norm als meetinstrument gebruikt. De NEN 7510 norm is een gezaghebbende sectorale uitwerking van artikel 13 Wbp; de in deze norm beschreven maatregelen worden door partijen uit het veld als adequaat gezien⁷, 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

NEN 7510 vereist het gebruik van unieke gebruikersidentificaties (ID) zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun handelingen.⁹

Uit het onderzoek is gebleken dat op de huisartsenpost gebruik wordt gemaakt van een (niet op naam gestelde) UZI-leenpas in geval een UZI-pas op naam defect is. Met zo’n niet op naam gestelde UZI-leenpas kunnen patiëntgegevens worden opgevraagd uit het huisartsinformatiesysteem (HIS) van een aangesloten huisarts via de OZIS-ring.

Hiermee wordt niet voldaan aan het vereiste dat elke gebruiker uniek wordt geïdentificeerd. Niet is gebleken dat maatregelen zijn getroffen om de gebruiker van de UZI-leenpas te koppelen aan zijn of haar handelingen.

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.

Logging

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.

Inzake logging is geen overtreding geconstateerd.

3. Conclusie voorlopige bevindingen

Met een niet op naam gestelde UZI-leenpas kunnen patiëntgegevens worden opgevraagd uit het huisartsinformatiesysteem (HIS) van een bij de huisartsenpost Enschede aangesloten huisarts.

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.

4. Schriftelijke zienswijze HDT-Oost

Constatering CBP

Met een niet op naam gestelde UZI-leenpas kunnen patiëntgegevens worden opgevraagd uit het huisartsinformatiesysteem (HIS) van een bij de huisartsenpost Enschede aangesloten huisarts. Daarbij is niet gebleken dat maatregelen zijn getroffen om de gebruiker van de UZI-leenpas te koppelen aan zijn of haar handelingen.

Reactie HDT-Oost

(1) Sinds 1 januari 2013 wordt geen gebruik meer gemaakt van de OZIS-koppeling tussen de HAP en de huisartsenpraktijken. De enige wijze waarop gegevens vanuit huisartsenpost Enschede nu nog bij een huisartsenpraktijk opvraagbaar zijn is via het Landelijk Schakelpunt, waarbij een opvraging alleen mogelijk is indien een huisarts zijn eigen UZI-pas op naam gebruikt.

(2) Er zijn wel degelijk maatregelen getroffen om de gebruiker van de UZI-leenpas te koppelen aan zijn of haar handelingen.¹⁰

5. Reactie CBP

¹⁰ Deze maatregelen zijn door HDT-Oost gedocumenteerd.

De voorlopige bevindingen dienen te worden gecorrigeerd naar aanleiding van hetgeen HDT-Oost heeft opgemerkt ten aanzien van de maatregelen om de gebruiker van de UZI-leenpas te koppelen aan zijn of haar handelingen (reactie HDT-Oost (2)). Deze maatregelen, waarmee wordt bereikt dat gebruikers kunnen worden gekoppeld aan zijn of haar handelingen, zijn echter op zichzelf onvoldoende om te kunnen spreken van unieke gebruikersidentificaties (ID), waardoor ondanks deze maatregelen op dit punt toch sprake was van overtreding van artikel 13 Wbp.

Overigens worden de constatering 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 HDT-Oost, aannemelijk dat de overtreding per 1 januari 2013 is beëindigd.

6. Definitieve conclusies

Het CBP stelt vast dat ten tijde van het onderzoek met een niet op naam gestelde UZI-leenpas patiëntgegevens konden worden opgevraagd uit het huisartsinformatiesysteem (HIS) van een bij de huisartsenpost Enschede aangesloten huisarts.

Hiermee werd 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 was ten tijde van het onderzoek sprake van overtreding van artikel 13 Wbp.

Op basis van de maatregelen die HDT-Oost inmiddels heeft getroffen concludeert het CBP dat de geconstateerde overtreding van artikel 13 Wbp thans is beëindigd.

Het College bescherming persoonsgegevens,
Voor het College,

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