

COLLEGE BESCHERMING PERSOONSgegevens

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKAADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

AAN NICTIZ

Postbus 262
2260 AG LEIDSCHENDAM

DATUM 17 januari 2008

ONS KENMERK z2007-01524

CONTACTPERSOON

UW BRIEF VAN 12 november 2007

UW KENMERK RdB/TH/07273

ONDERWERP EPD - intelligente logging

Geachte

In uw brief van 12 november 2007 nodigt u het CBP uit deel te nemen aan het overleg inzake toezicht op basis van intelligente logging.

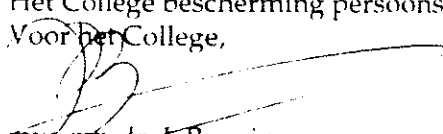
Zoals in de bespreking van 2 juli 2007 van de zijde van het CBP reeds is aangegeven zal het CBP niet deelnemen aan dit overleg.

Intensieve bemoeienis met de uitwerking van de logging past niet bij de toezichtsrol zoals het CBP deze wenst in te vullen: de verantwoordelijke in de zin van art. 1 sub d Wet bescherming persoonsgegevens dient er zelf voor te zorgen dat onrechtmatige toegang wordt voorkomen, primair door een goede autorisatie en aanvullend met behulp van logging. Het is dus aan de verantwoordelijke om de logging zo in te richten dat deze effectief bijdraagt aan de toegangsbeveiliging. Het CBP ziet er vervolgens op toe dat de verantwoordelijke in dit opzicht adequate maatregelen heeft genomen. Bovendien pleit het CBP, gezien de omvang van de verwerking en de gevoeligheid van de gegevens, zoals eerder aangegeven (zie onze brief van 14 juni 2007 aan het ministerie van VWS, kenmerk z2007-577, Bijlage p. 7-8), voor specifiek toezicht op het EPD.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

Het College bescherming persoonsgegevens,
Voor het College,


mw. mr. dr. J. Beuving
collegelid

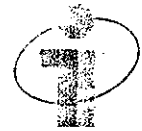
copie: - ministerie van VWS
- IGZ

22006-00319

College Bescherming Persoonsgegevens

13 NOV. 2007

Ontvangen



NICTIZ

Nationaal ICT Instituut in de Zorg

Postadres: Postbus 267
2314 AS Leidschendam

Verkeeradres: Tuingang 11
3720 XZ Leidschendam

Telefoon: 071 517 110
Fax: 071 517 147

E-mail: info@nictiz.nl
Internet: www.nictiz.nl

College Bescherming Persoonsgegevens (CBP)
T.a.v. mevrouw mr. dr. J. Beuving
Postbus 93374
2509 AJ DEN HAAG

Leidschendam, 12 november 2007
Ref.: RdB/TH/07273

Betreft: Autorisatie

Geachte mevrouw Beuving,

Bij brief van 18 september 2007 heeft u NICTIZ – met verwijzing naar de brief van NICTIZ van 23 mei 2006 – gevraagd of er inmiddels meer gedetailleerde informatie beschikbaar is over de autorisatieregels voor EMD en WDH dan beschreven in de betrokken modelrichtlijnen. Hierbij bericht ik u over de voortgang.

In het algemeen gelden er een aantal generieke, cumulatieve, voorwaarden bij het landelijk elektronisch patiëntendossier (EPD), waarvan EMD en WDH de eerste hoofdstukken zijn.

Ten eerste is alleen met de UZI-pas – een naar de stand van de techniek zeer hoogwaardig identificatie- en authenticatiemiddel - toegang mogelijk.

Ten tweede kan en mag per EPD-hoofdstuk alleen de door de betreffende beroepsgroep vastgestelde set met voor die behandeling noodzakelijk gegevens worden uitgewisseld.

Ten derde zijn er per EPD-onderdeel, afhankelijk van de specifieke context, procedurele autorisatierichtlijnen vastgesteld.

In aanvulling op deze drietrapsraket wordt het vertrouwensmodel van het EPD gecompleteerd met vereisten voor goed beheerde zorgsystemen, de informatiebeveiligingsnormen (zoals de NEN 7510), intelligente loggingsanalyse, toezicht en communicatie over wat en waarom (patiënt)gegevens worden verwerkt en welke mogelijkheden er zijn om via onder andere een klantenloket gebruik te maken van de bestaande patiëntenrechten.

Naar aanleiding van het bij u bekende - recent door NICTIZ uitgevoerde - haalbaarheidsonderzoek naar autorisatie op behandelrelatie wordt daar nu de controle op inschrijving als generieke maatregel aan toegevoegd.

De invulling van aanvullende autorisatierichtlijnen per EPD-onderdeel dienen in de context van dat EPD-onderdeel gezien te worden. Deze context wordt onder andere bepaald door variabelen als: voorspelbare/niet voorspelbare zorg en spoed of geen spoed.



Voor EMD/WDH zijn naast de controle op inschrijving als recente aanvulling vooralsnog geen nadere maatregelen voorzien in verband met de onvoorspelbaarheid van het gebruik deze gegevens. In hoeverre de bestaande autorisatierichtlijnen voor EMD en WDH in de praktijk adequaat zijn, zal overigens aan de orde komen bij de aanstaande evaluatie van de huidige pilots met EMD en WDH.

Voor nieuwe onderdelen van het EPD, waarbij het zorggebruik wel van te voren te voorzien is, zoals e-diabetes, zijn nadere maatregelen goed voorstelbaar. De mogelijkheden voor meer maatwerk bij autorisatie per EPD-onderdeel worden op dit moment door NICTIZ in samenwerking met VWS en de NPCF onderzocht in het project Autorisatie op maat. Ook zullen per nieuw EPD-onderdeel afzonderlijke, bij de context passende, autorisatierichtlijnen opgesteld met de beroepsgroepen, de NPCF et cetera.

Controle op inschrijving zie ik overigens als een zeer waardevolle aanvulling omdat dit de behandelrelatie benadert.

Ten aanzien van de rol voor de patiënt bij digitale autorisatie op afstand moet ik helaas vaststellen dat de komst van de eNIK opnieuw is vertraagd. NICTIZ en VWS overwegen nu in pilots DigiD+ te beproeven als authenticatiemiddel voor de patiënt. De voorbereidingen worden inmiddels getroffen.

Voorts bent u met VWS nader in overleg over autorisatie op de behandelrelatie. Ik ben daar nauw op aangesloten.

Tot besluit wijs ik u op het overleg inzake toezicht op basis van intelligente logging. Op dit moment nemen de IGZ, VWS en NICTIZ aan dit overleg deel. Graag nodig ik wederom het CBP – mede namens de IGZ en VWS – uit om aan dit overleg deel te nemen.

Ik ga ervan uit dat ik u hierbij voldoende heb geïnformeerd.

Met vriendelijke groet,