



COLLEGE BESCHERMING PERSOONSGEGEVENS

MEMO

AAN

DATUM 25 augustus 2008
NUMMER z2007-1525

KOPIE AAN

VAN

ONDERWERP sluiten zaak

Hetgeen CBP bij NICTIZ trachtte aan te kaarten is inmiddels opgepakt door VWS. Zie verder z2008-1021.

Deze zaak kan hiermee worden gesloten.

2
Res

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 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

AAN NICTIZ

Postbus 262
2260 AG LEIDSCHENDAM

DATUM 27 maart 2008

ONS KENMERK z2007-01525

CONTACTPERSOON

UW BRIEF VAN 12 november 2007

UW KENMERK RdB/TH/07273

ONDERWERP DigiD

Geachte!

In uw brief van 12 november 2007 schrijft u dat NICTIZ en VWS overwegen in pilots "DigiD+" te proberen als authenticatiemiddel voor de patiënt bij de toegang tot zijn epd.

In de vakpers zijn twijfels geuit over de kwaliteit van DigiD¹. Dit is voor het College bescherming persoonsgegevens (CBP) aanleiding geweest vragen over DigiD te stellen aan GBO Overheid (zie bijgaande brief van 20 maart 2008).

Graag zou het CBP in dit verband van u vernemen hoe de (voorlopige) keuze voor "DigiD+" is onderbouwd gezien de eisen die Wbp en WGBO stellen aan de beveiliging van medische persoonsgegevens.

Hoogachtend,

Het College bescherming persoonsgegevens,
Voor het College,



mw. mr. dr. J. Beuving
collegelid

¹Zie Jacobs, Jochems "DigiD en privacy" in Automatisering gids 19-10-2007

3
gea

MEMO

AAN

datum 27 december 2007

NUMMER z2007-1525, z2006-1363

KOPIE AAN

VAN

ONDERWERP DigiD in de zorg

Recent is het CBP op de hoogte gesteld van twee toepassingen van DigiD in de zorg, t.w.:

1. concept-brief van Flevoziekenhuis van 20 december 2007, waarin men aangeeft dat men DigiD in gebruik heeft genomen voor de beveiliging van hun online-afsprakenstelsel @pointment (Bijlage I).
2. brief van NICTIZ 12 november 2007 waarin directeur Van Boven schrijft: "NICTIZ en VWS overwegen nu in pilots DigiD+ te proberen als authenticatiemiddel voor de patiënt [bij toegang tot zijn epd]" (Bijlage II).

De toepassing van DigiD bij Flevoziekenhuis vloeit voort uit kritiek van het CBP op de beveiliging van hun online afsprakenstelsel @Pointment (z2005-1372) en vindt plaats in het kader van een door VWS gereguleerde pilot. De (voorgestelde) inzet van DigiD+ bij toegang tot het epd door de patiënt is het gevolg van het feit dat de introductie van de eNIK ernstig is vertraagd.

Beide tekenen wijzen onmiskenbaar op een bredere toekomstige inzet van DigiD in de zorg.

Bij Flevoziekenhuis gaat het voornamelijk niet om zeer gevoelige gegevens; bij het epd is dit uiteraard wel het geval.

DigiD is tot dusver niet door het CBP beoordeeld. Recent zijn twijfels gerezen over de kwaliteit van DigiD¹.

De organisatie GBO Overheid is verantwoordelijk voor DigiD. Het CBP heeft een contactpersoon bij deze organisatie.

Voorstel

GBO Overheid

Vragen om (schriftelijk) te reageren op de kritiek van Jacobs/Jochems.

¹Zie Jacobs/Jochems "DigiD en privacy" in Automatisering gids 19-10-2007

datum 27 december 2007
nummer z2007-1525, z2006-1363

Flevo

Aangeven dat met de in de brief van 20 december 2007 beschreven maatregelen tegemoet is gekomen aan de bezwaren van het CBP (uit z2005-1372). Voorts signaleren dat bij eventuele toekomstige uitbreiding van de gegevensset de beveiligingsmaatregelen – waaronder de toepassing van DigiD - opnieuw moeten worden overwogen (de balans van art. 13 WBP tussen mate van beveiliging en risico van de verwerking).

Bevestigen dat wij op de hoogte worden gesteld van de resultaten van de pilot, en dat daarbij ook aandacht wordt besteed aan het aspect bescherming persoonsgegevens.

Informeren dat vragen zijn gesteld aan GBO Overheid.

NICTIZ/VWS

Vragen of de keuze voor DigiD+ onderbouwd is gezien de eisen die WBP en WGBO stellen aan de beveiliging.

Informeren dat vragen zijn gesteld aan GBO Overheid.



Afdeling:
Doorkiesnr.:
Uw ref.:
Onze ref: DvB07154/mkb
Datum: 20 december 2007

College Bescherming Persoonsgegevens

Postbus 93374
2509 AJ DEN HAAG

Betreft: ingebruikname DigiD

Geachte

Conform mijn toezegging aan u in eerdere correspondenties bericht ik u hierbij dat het Flevoziekenhuis op vrijdag 23 november 2007 DigiD in het kader van een pilot formeel in gebruik heeft genomen voor de beveiliging van haar afsprakenportal @-pointment.

Concreet betekent dit dat alle gebruikers van @-pointment vanaf dat moment dienen te beschikken over een gebruikersnaam en een wachtwoord. Hierbij kunnen de gebruikers van @-pointment zelf een gebruikersnaam en een wachtwoord kiezen, maar indien men beschikt over een DigiD dan kan men ook hiervan gebruik maken. De patiënt heeft dus de keuze uit 2 mogelijkheden.

Indien men niet kiest voor DigiD wordt gevraagd een gebruikersnaam en een wachtwoord te kiezen. Naar het opgegeven mailadres wordt een bericht gestuurd waarmee de patiënt zijn of haar account kan activeren. Zolang dit niet is gebeurd heeft men geen toegang tot @-pointment en kan men geen afspraken maken, inzien, wijzigen of annuleren.

Indien men kiest voor DigiD dan kan men inloggen met de (reeds in het verleden aangevraagde) gebruikersnaam en het wachtwoord van zijn of haar DigiD. Deze gebruikersnaam en wachtwoord wordt middels een verbinding door de DigiD-organisatie (GBO.overheid) geverifieerd en indien juist akkoord bevonden. Hierna heeft de gebruiker toegang tot de applicatie. Op de site wordt ook informatie gegeven over het gebruik van DigiD. Indien men niet over een DigiD beschikt wordt de mogelijkheid geboden om er een aan te vragen.

Zoals gezegd betreft deze introductie van DigiD vooralsnog een pilot. Deze pilot voeren wij uit in nauw overleg met VWS, die het Flevoziekenhuis in de gelegenheid heeft gesteld als eerste zorginstelling van DigiD gebruik te maken. Na beëindiging van de pilot (voorjaar 2008) vindt een evaluatie plaats. Van de resultaten hiervan zullen wij u op de hoogte stellen.

Ik vertrouw u hiermee voldoende te hebben geïnformeerd en wil u bedanken voor uw advies en medewerking om onze dienstverlening verder te verbeteren.

Met vriendelijke groet,
FLEVOZIEKENHUIS

MEMO

AAN

DATUM 29 november 2007

NUMMER z2007-1020

KOPIE AAN

VAN

ONDERWERP brief van NICTIZ 12 november 2007

1. Deze zaak staat op jouw "van 3 naar 2 lijst". Ik laat het verder aan jou of onderstaande issues met het College(lid) en/of anderen dienen te worden besproken.

2. Men verwijst naar de bestaande autorisatierichtlijnen WDH en EMD. Raadpleging van de NICTIZ website leerde mij dat deze dateren van 2005. Deze richtlijnen zijn eerder voorgelegd aan het CBP (z2005-448 en z2005-1363). In beide richtlijnen wordt geen helder beeld geschetst van de wijze waarop de autorisatie feitelijk is vormgegeven. (zie de brief van [] aan NICTIZ van 21 maart 2006 (z2006-319)).

Vraag: Nemen wij genoeg met dit antwoord?

Mijn advies: Nee, maar aandringen heeft thans om meerdere redenen geen zin. Dus voor dit moment: ja. Zaak sluiten.

3. Van Boven schrijft: "NICTIZ en VWS overwegen nu in pilots DigiD+ te beproeven als authenticatiemiddel voor de patiënt [bij toegang tot zijn epd]".

Vraag: Wil het CBP hierop reageren?

Mijn advies: Ja. Er zijn twijfels aan de kwaliteit van DigiD¹. DigiD is bezig met een gestage opmars, ook in de zorg (zie ook z2006-1363 (Flevoziekenhuis)): **Nieuwe zaak.**

4. Van Boven nodigt "wederom het CBP – mede namens de IGZ en VWS – uit om aan [het] overleg [inzake toezicht op basis van intelligente logging] deel te nemen."

Met instemming van het College heb ik eerder mondeling aangegeven dat het CBP hier niet op in gaat.

Vraag: Hoe reageren wij op deze uitnodiging?

Mijn advies: CBP wil controle vooraf, niet achteraf; daarnaast ontbreekt wellicht prioriteit en past het minder goed bij de nieuwe positionering CBP. Daarom uitnodiging wederom

¹ Zie Jacobs/Jochems "DigiD en privacy" in Automatisering gids 19-10-2007



COLLEGE BESCHERMING PERSOONSGEGEVENS

DATUM 29 november 2007

NUMMER z2007-1020

afslaan. Mijn voorstel is wel dit schriftelijk te doen met afschrift aan IGZ en VWS. Nieuwe zaak)

NICTIZ
Nederlandse
Instituut voor
de Toekomst van de
Zorg

NICTIZ

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 voorsnog 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,