

JESC

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 Ministerie van VWS

DATUM 26 augustus 2008

ONS KENMERK z2008-01021

CONTACTPERSOON

Postbus 20350
2500 EJ 'S-GRAVENHAGE

UW BRIEF VAN 7 augustus 2008

UW KENMERK MEVA/I&I-2865877

ONDERWERP Identificatie en authenticatie bij toegang patiënt tot het EPD

Geachte

U heeft het College bescherming persoonsgegevens (CBP) verzocht aan te geven of de in uw brief van 7 augustus 2008 vervatte uitgangspunten voor de beveiliging van de toegang tot het epd door de patiënt door het CBP worden onderschreven.

Op grond van artikel 13 Wet bescherming persoonsgegevens (Wbp) dient de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beschermen tegen verlies of enige vorm van onrechtmatige verwerking.

Bij de beoordeling welke maatregelen moeten worden getroffen dient rekening te worden gehouden met een aantal aspecten, waaronder de risico's die de verwerking en de aard van de te beschermen gegevens met zich brengen. Hierover heeft de Registratiekamer (de voorganger van het CBP) een publicatie uitgebracht. Deze publicatie, "Beveiliging van persoonsgegevens" (A&V-studie 23, april 2001) is te vinden op de website van het CBP (www.cbpweb.nl), via "nieuws en publicaties", "publicaties", "A&V-studies"). In casu is sprake van persoonsgegevens betreffende de gezondheid, waarop het medisch beroepsgeheim van toepassing is. Deze gegevens vallen in de hoogste risicoklasse, risicoklasse III. Zoals in A&V-studie 23 is beschreven (zie pagina 28) moet voor de beveiliging van persoonsgegevens in risicoklasse III worden voldaan aan de hoogste normen.

Het CBP heeft in zijn advies aan uw minister inzake wijziging Wet gebruik BSN in de zorg van 14 juni 2007 in dit verband het volgende opgemerkt:

"Of de patiënt rechtstreeks (elektronisch) zijn epd moet kunnen raadplegen, is afhankelijk van de vraag of dat praktisch mogelijk is. Het recht van de betrokkene op toegang tot de gegevens, bijvoorbeeld op grond van artikel 35 Wbp, houdt niet noodzakelijk altijd rechtstreekse toegang in. Rechtstreekse toegang kan echter aanzienlijk bijdragen aan het vertrouwen in een EPD-systeem. Uit het oogpunt van gegevensbescherming is veilige elektronische identificatie en authenticatie een voorwaarde voor de toekenning van rechtstreekse toegang, zulks om onbevoegden de toegang te beletten. Met een smartcard kan correcte elektronische identificatie van patiënten aanzienlijk worden bevorderd."

College bescherming persoonsgegevens

Ministerie van Volksgezondheid, Welzijn en Sport

08 AUG. 2008

Ontvangen

VWS

College Bescherming Persoonsgegevens
Postbus 93374
2509 AJ Den Haag

Ons kenmerk
MEVA/I&I-2865877

Inlichtingen bij

Doorkiesnummer

Den Haag
07 AUG 2008

Onderwerp
Identificatie en authenticatie bij toegang
patiënt tot het EPD

Bijlage(n)

Uw brief

Vanuit diverse kanten wordt er aangedrongen op elektronische toegang voor zorgconsumenten tot de eigen medische gegevens in het EPD. Nu de invoering van de eerste delen van het EPD in de koploperregio's is gerealiseerd en de start van de landelijke uitrol voor de deur staat, is er een noodzaak om deze toegang daadwerkelijk vorm te geven. Het gaat hierbij om de directe toegang voor de zorgconsument tot zijn/haar EPD via het internet.

Eén van de onderdelen waaraan invulling moet worden gegeven betreft de identificatie en authenticatie van de zorgconsument. In eerdere stadia werd uitgegaan van de komst van de elektronische Nederlandse identiteitskaart (eNIK) als identificatie- en authenticatiemiddel voor de zorgconsument. Uit gesprekken met het Ministerie van BZK is duidelijk geworden dat de eNIK momenteel als niet opportuun wordt gezien. Verwachting is dan ook dat deze de komende jaren niet gereed zal zijn.

Op 11 juni jl. heeft een verkennende workshop plaatsgevonden op het Ministerie van VWS in het kader van 'toegang patiënt tot het EPD'. Aanwezigen waren vertegenwoordigers van het Ministerie van BZK, het CBP, de NPCF, Nictiz en het Ministerie van VWS. Bij het verkrijgen van toegang tot zorginhoudelijke informatie is het overbodig om te melden dat hierbij het hoogst beschikbare beveiligingsniveau in acht moet worden genomen. Tijdens de workshop is dan ook met name gesproken over de minimale eisen ten aanzien van beveiliging voor identificatie en authenticatie van de zorgconsument. Wat betreft het EPD kan onderscheid worden aangebracht in een vijftal functionaliteiten in het kader van toegang voor de patiënt:

- Totaal bezwaar;
- Uitsluiten op naam & beroepsgroep;
- Inzage in verwijzindex;
- Inzage in logginggegevens;
- Inzage in medische gegevens.

Ministerie van Volksgezondheid, Welzijn en Sport

Blad

2

Kenmerk

MEVA/I&I-2865877

VVFU

Voor de eerste twee functionaliteiten, te weten totaal bezwaar en het uitsluiten van zorgverleners op naam en/of beroepsgroep, is tijdens de workshop d.d. 11 juni geconstateerd dat volstaan kan worden met een lager niveau van beveiliging. Dit vanwege het feit dat deze gegevens niet onder het medisch beroepsgeheim vallen. Voor de overige drie functionaliteiten daarentegen is aangegeven dat voldaan moet worden aan het hoogst beschikbare beveiligingsniveau. Dit houdt in dat ten aanzien van het toegangsmiddel een 2-factor authenticatie van belang zal zijn, zoals bij DigiD met sms verificatie, en ten aanzien van het uitgifteproces dat dit face-to-face zal moeten plaatsvinden.

Graag verneem ik van u of wij voor het realiseren van de toegang tot het EPD voor de zorgconsument inderdaad uit kunnen gaan van de hierboven omschreven beveiligingseisen en toebehorende authenticatiemiddelen en uitgifteproces. Gelet op de noodzaak om de zorgconsument elektronische toegang te geven tot zijn/haar medische gegevens wordt hoge prioriteit gegeven aan dit traject. Daar waar mogelijk zal een versnelling van toepassing zijn. In dit kader zou het prettig zijn om op korte termijn van u een antwoord te ontvangen. Parallel hieraan zal ik opdracht geven tot een onafhankelijk advies rondom de technische beveiligingsaspecten van bovenstaand voorstel.

Hoogachtend,

de Directeur-Generaal Langdurige Zorg,

drs. M.J. Boereboom

