COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Prins Clauslaan 20
TEL 070 - 381 13 00 FAX 070 - 381 13 01 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

AAN Ministerie van VWS

DATUM 10 januari 2006
ONS KENMERK z2005-0814
CONTACTPERSOON

UW BRIEF VAN
UW KENMERK

ONDERWERP pseudonimisering DIS

In uw brief vraagt u het College bescherming persoonsgegevens (CBP) advies over het toepassen van pseudonimisering van medische persoonsgegevens in het DBC Informatiesysteem (DIS). De daartoe gekozen aanpak is neergelegd in de notitie “Beschrijving gebruik pseudo-identiteiten binnen het Diagnose Behandel Combinatie Informatiesysteem – structurele situatie” door Stichting IVZ (november 2005).

Naar het oordeel van het CBP beschrijft de notitie van IVZ een correcte toepassing van de pseudonimiseringsoplossing. Daardoor mag redelijkerwijs worden aangenomen dat in het DIS geen sprake is van verwerking van persoonsgegevens, mits aan een aantal – verder te stellen - voorwaarden is voldaan.

DIS – drie doelen

De taak van het DIS is het verzamelen en opslaan van DBC-gegevens van alle Nederlanders in een centrale database en deze al dan niet bijgewerkte informatie vervolgens verstrekken aan diverse afnemers.

Deze verwerking dient volgens de notitie drie doelen (tussen haakjes staan de betrokken afnemers):
risicoverevening (CVZ);
statistiek (CBS), en
DBC-onderhoud (CTG / Zaio).

Doel 1: Risicoverevening(CVZ)

Voor het uitvoeren van de de risicoverevening is het niet noodzakelijk dat persoonsgegevens worden verwerkt. Wèl is het in de gekozen systematiek nodig dat van elkaar in de loop der tijd opvolgende DBC’s kan worden vastgesteld dat zij betrekking hebben op één en dezelfde persoon. Daarbij is het echter niet nodig dat ook bekend is welke persoon dit is.

Doel 2: Statistiek (CBS)

Het CBS verlangt dat met het oog op de samenstelling van statistische informatieproducten waarin kruisverbanden worden gelegd tussen gezondheidsgegevens en andersoortige gegevens, zoals over welstand of woonsituatie, de DBC-gegevens uit het DIS kunnen worden gekoppeld met persoonsgegevens die reeds bij haar aanwezig zijn.

Doel 3: DBC-onderhoud (CTG/Zaio)

Voor DBC-onderhoud zijn geen persoonsgegevens of pseudo-identiteiten vereist.

Gekozen aanpak (op hoofdlijnen)

Bij de periodieke aanlevering van DBC-informatie worden de identificerende kenmerken van de behandelde persoon door de zorgaanbieder omgezet in een pre-pseudo-identiteit, die in de Trusted Third Party (TTP) nogmaals wordt versleuteld tot een pseudo-identiteit. Bij DIS zijn alle DBC's die betrekking hebben op deze persoon uitsluitend gekoppeld aan deze pseudo-identiteit. Ook de afnemers van DIS beschikken derhalve – voor zover noodzakelijk - uitsluitend over een pseudo-identiteit.

Voor het CBS is een bijzondere situatie gecreëerd. Aan het CBS wordt namelijk – als enige afnemer- de sleutel verstrekt waarmee het de pseudo-identiteiten alsnog kan identificeren. Daarbij wordt tussen DIS en CBS nogmaals versleuteld met als effect dat het onmogelijk is om met behulp van de sleutelinformatie bij het CBS de versleuteling bij het DIS te kraken.

Beoordeling

De gekozen aanpak beschrijft een correcte toepassing van de pseudonimiseringsoplossing binnen het DIS.

De verstrekking van de sleutel aan het CBS doet hieraan niet af. Door nogmaals te versleutelen tussen DIS en CBS ontstaat geen extra risico dat de versleuteling bij het DIS wordt gekraakt. Bovendien is het achterliggend privacyrisico gering. De Wet op het CBS verbiedt het CBS immers persoonsgegevens verder te verstrekken of openbaar te maken. Het CBS heeft daarnaast het wettelijk recht deze gegevens op te vragen.

Eén en ander neemt niet weg dat het DIS zowel qua omvang, dekking als inhoud een van de meest risicovolle verwerkingen binnen Nederland zal zijn. Door pseudonimisering onttrekt deze verwerking zich aan stringente wettelijke normen. Dit maakt dat bij de verdere uitwerking van de pseudonimisering van het DIS de hoogst denkbare maatstaven dienen te worden gehanteerd.

Conclusie

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1 sub a Wet bescherming persoonsgegevens). Uitgangspunt is dat een persoon identificeerbaar is indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

Bij toepassing van pseudonimisering is geen sprake van verwerking van persoonsgegevens, indien aan de volgende voorwaarden is voldaan:

a. er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de zorgaanbieder;
b.er zijn technische en organisatorische maatregelen genomen om herhaalbaarheid van de versleuteling ("replay attack") te voorkomen;
c. de verwerkte gegevens zijn niet indirect identificerend, en
d. in een onafhankelijk deskundig oordeel (audit) wordt vooraf en daarna periodiek vastgesteld dat aan de voorwaarden a, b en c is voldaan.

Naar het oordeel van het CBP mag redelijkerwijs worden aangenomen dat de notitie van IVZ een correcte uitwerking vormt van de voorwaarden a. en b.

Tenslotte

Zodra niet (meer) aan de bovengenoemde voorwaarden wordt voldaan, is sprake van persoonsgegevens en zijn WBP en medisch beroepsgeheim weer onverkort van toepassing ten aanzien van die gegevens. Daarbij kunnen ook technische ontwikkelingen een rol spelen. Wat bij een bepaalde stand van de techniek immers als anoniem, want redelijkerwijs niet tot een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen – bijvoorbeeld op het gebied van de cryptografie - alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding. Nu voor verwerking van persoonsgegevens in DIS geen rechtsgrond bestaat, zou in dat geval sprake zijn van een onrechtmatige gegevensverwerking. Het blijven voldoen aan de gestelde voorwaarden vereist dus continue inspanning.

De vormgeving van de TTP vormt een belangrijk aandachtspunt in de verdere uitvoering. De onafhankelijkheid, deskundigheid en betrouwbaarheid van de TTP dienen boven elke twijfel verheven te zijn.

Soms leiden gegevens niet direct tot identificatie van een bepaald persoon maar kunnen de gegevens via nadere stappen, bijvoorbeeld door combinatie met andere gegevens, in verband worden gebracht met een bepaalde persoon. Dit soort gegevens heten indirect identificerende gegevens.
Bij de verdere uitwerking zal reeds in een vroeg stadium – in de fase systeemontwerp en bij de definitie van de gegevenssets - dienen te worden onderzocht of de verwerkte gegevens niet indirect identificerend zijn. Dit onderzoek dient verderop in de levensscyclus van het DIS bij wijziging van de gegevenssets en overigens periodiek te worden herhaald.

Deze drie punten zijn, naast andere, belangrijke toetsingscriteria bij de uit te voeren audits.

Met uw ministerie is afgesproken dat de gegevensverstrekking van zorgaanbieders aan DIS anoniem - d.w.z. de (direct en indirect) identificerende kenmerken zijn uit de bestanden verwijderd – plaatsvindt tot de onderhavige pseudonimiseringsoplossing volledig is gerealiseerd.

Het CBP gaat er daarbij van uit, dat deze afspraak wordt verwerkt in de regelingen van CTG / Zaio en ook overigens afdoende wordt gecommuniceerd (zie ook onze brieven van 13 en 22 december 2005, kenmerk z2005-1385).

Hoogachtend,

mw. mr. dr. J. Beuving
Collegelid