

Bijlage bij de brief van het College bescherming persoonsgegevens van 14 juni 2007.

Advies van het College bescherming persoonsgegevens (CBP) over het voorstel tot wijziging van de Wet gebruik BSN in de zorg.

1. Inleiding

Op 20 april 2007 ontving het College bescherming persoonsgegevens (CBP) van het ministerie van VWS de adviesaanvraag inzake het wetsvoorstel tot wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de landelijke elektronische informatie-uitwisseling in de zorg (verder te noemen: het wetsvoorstel). Dit wetsvoorstel regelt het Elektronisch patiëntendossier (EPD), de daarvoor benodigde infrastructuur en de daarbij geldende randvoorwaarden.

Vanwege de grote maatschappelijk betekenis van het EPD en de aanzienlijke risico's die met invoering ervan zijn gemoeid, is een goede wettelijke regeling van essentieel belang.

1.1. Inhoud van het wetsvoorstel

Het wetsvoorstel beschrijft de taken en functies van het Landelijk Schakelpunt (LSP), de aldaar aanwezige verwijzindex en geeft een opsomming van de gegevens in deze verwijzindex (art. 13a, lid 1 en 2).

Zorgverleners zijn verplicht aan te sluiten op het LSP (art. 13d lid 1 sub a) en wisselen via het LSP onderling patiëntgegevens uit (art. 13d lid 1 sub b-f), "voor zover dat noodzakelijk is met het oog op een goede behandeling of verzorging van de patiënt" (art. 13d lid 2).

Art. 13f beperkt de toegang tot het EPD tot "beroepsbeoefenaars" zoals gedefinieerd in art. 1 sub q. Van alle opvragingen en mutaties wordt een logging bijgehouden (art. 13b lid 2).

In het wetsvoorstel wordt nadere invulling gegeven aan de informatieverstrekking aan de betrokkene als beschreven in Hoofdstuk 5 van de Wet bescherming persoonsgegevens (Wbp) (art. 13e lid 1) alsmede aan de rechten van de betrokkene als beschreven in Hoofdstuk 6 van de Wbp (art. 13a lid 2, 13c, 13e lid 3 en 4).

In verband hiermee wordt specifiek ten behoeve van de "cliënt" (terminologie wetsvoorstel) een "klantenloket" ingesteld (art. 13i).

De patiënt wordt de mogelijkheid van een opt-out geboden (art. 13e lid 2 en 5). Men is dus niet verplicht "mee te doen" met het EPD.

Inspecteurs van IGZ mogen volgens het wetsvoorstel gegevens – waaronder persoonsgegevens – opvragen bij zorgverleners en het LSP in verband met het toezicht op de naleving van de Kwaliteitswet zorginstellingen voor wat betreft het EPD (art. 16).

Expliciet is opgenomen dat het wetsvoorstel geen lex specialis is t.o.v. de art. 7:454-458 BW (art. 13h).

Tenslotte beschrijft het wetsvoorstel ter uitvoering van art. 24 Wbp de gevallen waarin het UZI-nummer en -abonneenummer mogen worden gebruikt (art. 14 en 15). Deze nummers zijn zorgverlener-identificatienummers.

1.2 Opzet EPD

Er is gekozen voor decentrale opslag, dat wil zeggen dat het EPD is vormgegeven als een systeem dat toegang biedt tot de medische dossiers die berusten bij de zorgverlener.

Deze opzet sluit goed aan bij het medisch beroepsgeheim en bevordert het vertrouwen dat de patiënten in het systeem stellen: de zorgverlener blijft immers verantwoordelijk voor de gegevens en de vrees voor centrale opslag van gevoelige persoonsgegevens wordt bij voorbaat weggenomen.

Bij deze decentrale opslag, een model dat slechts door de toevoeging van zoekpaden een “systeem” wordt, blijft de bestaande documentatiestructuur van de gezondheidsgegevens bij de verschillende zorgverleners ongewijzigd. In hoeverre gegevens betreffende een patiënt in dit systeem kunnen worden opgezocht, is afhankelijk van de kwaliteit van de zoekfaciliteiten. In dit organisatiemodel blijft de zorgverlener/zorginstelling onverkort “verantwoordelijk” voor het dossier (meer bepaald het gedeelte van het EPD dat door hem/haar is aangemaakt).

De decentraal opgeslagen gegevens kunnen door een andere zorgverlener worden benaderd via de zogenaamde verwijzindex bij het LSP. In deze verwijzindex kan worden opgezocht bij welke zorgverleners zich informatie van een patiënt bevindt.

2. Beoordeling

De toepasselijke normen zijn helder beschreven in de Wbp en in art. 7: 454-457 Burgerlijk Wetboek (BW). Een adequate interpretatie van de relevante normen uit de Richtlijn 95/46/EG is bovendien gegeven in het recente “Working document on the processing of personal data relating to health in electronic health records (EHR)” van de Article 29 Data Protection Working Party (verder te noemen: WP29).¹

2.1. art. 7: 457 BW

Ingevolge art. 7:457 lid 1 BW verschaft een hulpverlener aan anderen dan de patiënt geen inlichtingen over de patiënt zonder diens toestemming, tenzij het bij of krachtens de wet bepaalde daartoe verplicht. Onder anderen dan de patiënt zijn niet begrepen degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst 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 (art. 7:457 lid 2 BW).

In het onderhavige wetsvoorstel is de verplichting geregeld voor zorgverleners om zich aan te sluiten op het LSP. Daarmee voorziet het wetsvoorstel in een doorbreking van het beroepsgeheim en een grondslag voor het verwerken van persoonsgegevens van de patiënt door het LSP, voor zover deze verstrekking noodzakelijk is met het oog op een goede behandeling of verzorging van de patiënt (art. 13d). Voor de verwerking van deze gegevens door het LSP is toestemming van de patiënt daarom niet (meer) vereist. De gegevensverwerking dient echter achterwege te blijven wanneer de patiënt daartegen bezwaar maakt.

2.2. Artikel 16 Wbp

¹ De WP29 is ingesteld ingevolge art. 29 van de Richtlijn 95/46/EG. Het is het onafhankelijke EU adviesorgaan inzake gegevensbescherming en privacy.

Het behoeft geen betoog dat de in het EPD-systeem opgenomen gegevens moeten worden beschouwd als persoonsgegevens betreffende iemands gezondheid in de zin van art. 16 Wbp. Deze gegevens vallen derhalve niet alleen onder de algemene regels van de Wbp, maar ook onder de extra bescherming van bijzondere persoonsgegevens zoals neergelegd in Hoofdstuk 2, Paragraaf 2 van de Wbp. Art. 16 Wbp verbiedt de verwerking van bijzondere persoonsgegevens behoudens de in voornoemde paragraaf genoemde uitzonderingen. Op de verwerking van medische persoonsgegevens zijn in dit kader de artikelen 21 en 23 Wbp van toepassing.

2.3. Artikel 21 Wbp

Aangezien de uitzonderingen van art. 21 lid 1 sub b t/m f Wbp hier evident niet aan de orde zijn, resteert uitsluitend de vraag of de uitzondering van art. 21 lid 1 sub a Wbp² op het EPD van toepassing kan zijn.

Het CBP constateerde reeds eerder dat de voorgenomen verwerking van patiëntgegevens door het LSP niet gebaseerd kan worden op de uitzondering van art. 21 lid 1 sub a Wbp (z2005-505 en z2005-878). Ook de WP29 komt in het eerder aangehaalde Working document na ampele overwegingen tot de conclusie dat een wettelijke grondslag voor een EPD is aangewezen.

Het CBP komt op grond van het bovenstaande tot de conclusie, dat voor het geheel van verwerkingen in het kader van het EPD art. 21 lid 1 sub a Wbp toepassing mist.

2.4. Artikel 23 Wbp

Een andere uitzondering op het verbod als bedoeld in art. 16 Wbp wordt gevormd door art. 23 Wbp. In art. 23 lid 1 sub e Wbp wordt de mogelijkheid geboden een dergelijke uitzondering bij wet te regelen, mits aan de volgende eisen wordt voldaan: zijn de betrokken gegevensverwerkingen noodzakelijk met het oog op een zwaarwegend algemeen belang en zijn passende waarborgen geboden ter bescherming van de persoonlijke levenssfeer?

2.4.1. Belang van het EPD

Het EPD heeft als doel patiëntgegevens, die berusten bij de behandelend arts, op elektronische wijze ter beschikking te stellen aan andere zorgverleners. Daarmee wordt de medische informatievoorziening op een hoger plan gebracht ten opzichte van de traditionele vormen van medische documentatie: er komt potentieel meer en betere informatie over de patiënt beschikbaar, waardoor de kwaliteit van de behandeling kan verbeteren.

Hiermee is het zwaarwegend algemeen belang reeds gegeven.

Daaraan doet niet af dat in de internationale praktijk tot dusver de EPD's nauwelijks van de grond zijn gekomen, en dat zij, voor zover invoering dan wel is gelukt, worden geteisterd door allerlei ernstige technische en operationele problemen. Dit gegeven doet immers geen afbreuk aan de

² Deze bepaling verklaart het verbod om persoonsgegevens betreffende iemands gezondheid te verwerken als bedoeld in artikel 16 niet van toepassing indien de verwerking geschiedt door hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening 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

potentie van een EPD, maar onderschrijft hoogstens de dwingende noodzaak van een zorgvuldige implementatie.

2.4.2. Passende waarborgen

In de context van gegevensbescherming moet echter worden onderstreept dat met een EPD-systeem niet alleen meer persoonsgegevens kunnen worden verwerkt, maar patiëntgegevens ook gemakkelijker toegankelijk kunnen worden gemaakt voor meer gebruikers dan voorheen.

Ook moet worden opgemerkt dat de elektronische medische informatie in een EPD-systeem - afgezien van de beschikbaarheid voor zorgverleners - in het algemeen de belangstelling kan wekken van derden, zoals verzekeraars en rechtshandavingsinstanties. Door het bijeenbrengen van medische informatie over een persoon uit verschillende bronnen, waardoor deze gevoelige informatie gemakkelijker en breder toegankelijk wordt, leidt een EPD-systeem wat de bescherming van persoonsgegevens betreft tot een nieuw risicoscenario, waardoor de schaal van mogelijk misbruik van medische informatie over individuen wordt vergroot.

Art. 23 lid 1 sub e Wbp verlangt dat bovenstaande risico's worden gepareerd door passende waarborgen ter bescherming van de persoonlijke levenssfeer. Beschouwing van het wetsvoorstel in het licht van deze eis leidt tot de volgende aandachtspunten:

- verantwoordelijkheid voor LSP;
- beveiliging – waaronder begrepen: autorisatie;
- de rechten van de patiënt;
- toezicht op het EPD.

2.5. Belangrijkste aandachtspunten bij dit wetsvoorstel

2.5.1. Verantwoordelijke LSP

Het LSP is als het ware de spin in het web van het Nederlands EPD-stelsel en vervult daarmee een cruciale rol. Uiteindelijk wordt door het LSP feitelijk toegang verschaft tot een dossier; alle essentiële elementen van beveiliging (beschikbaarheid, vertrouwelijkheid en integriteit) spelen daarbij een prominente rol, en het LSP dient daarom zowel technisch als organisatorisch excellent ingericht te zijn.

De bewering, dat in het LSP “louter uitvoerende taken (worden) verricht” (MvT p. 29) doet aan deze situatie bepaald geen recht.

Gezien het bovenstaande dient van meet af aan duidelijk te zijn wie verantwoordelijk (artikel 1 sub d Wbp) zal zijn voor het LSP. In het wetsvoorstel ontbreekt deze aanwijzing en de MvT (p.29) is op dit punt niet helder genoeg.

2.5.2. Beveiliging (inclusief autorisatie)

2.5.2.1. Algemeen

Op grond van artikel 13 Wbp moet de voor de verwerking verantwoordelijke passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Het beveiligingsniveau dient te worden afgestemd op de risico's van de verwerking en de aard van de te beschermen gegevens.

2.5.2.2. Toegang tot het EPD

Burgers zullen een EPD-systeem alleen aanvaarden als voor hen vaststaat dat het systeem vertrouwelijk omgaat met hun medische gegevens. Toegang tot de gegevens in een EPD moet in overeenstemming zijn met het hoofddoel van het EPD, namelijk een succesvolle medische behandeling door betere informatievoorziening.

Art. 13f beperkt de toegang tot het EPD tot "beroepsbeoefenaars". Dit begrip is gedefinieerd in art. 1 sub q en omvat de beroepsgroepen zoals genoemd in art. 3 en art. 34 Wet BIG. Art. 13d lid 2 bindt de toegang tot het EPD aan het doel van "een goede behandeling of verzorging van de patiënt".

Eén en ander is volledig in lijn met het aan het begin van deze paragraaf beschreven uitgangspunt, en betekent dat toegang tot de medische EPD-gegevens voor andere doeleinden niet is geoorloofd.

Vanuit het oogpunt van gegevensbescherming is het een essentieel vereiste dat de toegang voor onbevoegden wordt voorkomen. De beloofde voordelen van het EPD zijn echter alleen te realiseren indien het systeem voor bevoegde zorgverleners vrijwel onbeperkt beschikbaar is wanneer die zorgverleners de betrokken gegevens nodig hebben. Als wezenlijk beginsel moet derhalve gelden dat – naast de patiënt zelf – uitsluitend zorgverleners/bevoegde personeelsleden van een zorginstelling die op dat moment betrokken zijn bij de behandeling van de patiënt toegang mogen krijgen tot het EPD: tussen de patiënt en de zorgverlener die toegang wenst te krijgen tot diens EPD moet op dat moment een behandelrelatie bestaan (overeenkomstig art. 7: 457 BW).

Uit de MvT blijkt echter dat het bestaan van een behandelrelatie geen onderdeel vormt van de autorisatie bij het LSP. In plaats daarvan wordt logging van de transacties van de behandelaar en controle daarop voldoende geacht om misbruik te voorkomen.

Het is echter niet voldoende dat achteraf kan worden vastgesteld dat iemand zijn boekje te buiten is gegaan en onbevoegd toegang heeft verkregen tot een medisch dossier, nog daargelaten dat het waarschijnlijk onbegonnen werk is om al die loggegevens werkelijk te controleren.

In eerdere contacten tussen het ministerie van VWS en het CBP inzake het EPD heeft het CBP herhaaldelijk navraag gedaan naar de technische (on)mogelijkheden om een dergelijke autorisatie te realiseren. Daarbij heeft het CBP onder meer de suggestie gedaan een haalbaarheidsonderzoek te laten uitvoeren. Het ministerie van VWS is niet overgegaan tot het instellen van een dergelijk onderzoek waardoor voor het CBP niet is komen vast te staan dat bedoelde autorisatie technisch of anderszins onmogelijk is.

Gezien het feit dat een zorgverlener in het algemeen zonder meer in staat is de declaratie van een behandeling naar de patiënt of diens verzekeraar te sturen en gezien de algemeen bestaande praktijk dat bij een eerste contact tussen zorgverlener en patiënt de laatste wordt opgenomen in de administratie van de zorgverlener, is het aannemelijk dat deze relatie wel degelijk kan worden gelegd in het systeem.

Een geheel ander punt is of een geslaagde check op behandelrelatie in alle gevallen een voorwaarde moet zijn voor toegang tot iemands patiëntgegevens. In spoed- of noodgevallen waarin (nog) geen

behandelrelatie bestaat of kan worden aangetoond, kan, ook naar het oordeel van het CBP, toegang worden verleend tot het individuele dossier. In zulke gevallen dient dan een specifieke log worden aangemaakt waardoor op zulke transacties achteraf gericht toezicht mogelijk wordt.

2.5.2.3. Normering beveiliging

De normering van de beveiliging ontbreekt in het wetsvoorstel of is gedelegeerd. Ook in de MvT ontbreekt een concrete aanduiding van de voor het EPD geldende beveiligingsnormen, bijvoorbeeld in de vorm van een verwijzing naar de norm NEN 7510. Aldus ontbreekt voornamelijk het specifiek juridische kader voor de te treffen beveiligingsmaatregelen, waardoor het wetsvoorstel onvoldoende waarborgen biedt voor een goede beveiliging.

2.5.2.4. ZSP

Hoewel de ZSP (ZorgServiceProvider) wel een onderdeel vormt van de AORTA infrastructuur wordt hij niet in de wet genoemd. Voor zover bekend sluit de ZSP de zorgverleners aan nadat hij heeft gecontroleerd dat zij aan de aansluitvoorwaarden voldoen. Deze aansluitvoorwaarden hebben voor een belangrijk deel betrekking op beveiliging. De positie van de ZSP dient dus ook in het wetsvoorstel te worden geregeld.

2.5.2.5. Disciplinaire maatregelen bij onrechtmatige toegang

Het tuchtrecht voor zorgverleners zou moeten worden uitgebreid met effectieve sancties om overtreding van de EPD-toegangsregels tegen te gaan.

2.5.3. Rechten van de patiënt

2.5.3.1. Inzage en informatieplicht

De artikelen 13a lid 2, 13c lid 1, 13e lid 3 en 4 en 13i lid 1 sub b onder 1 hebben betrekking op inzage door de patiënt van zijn epd-gegevens en van de loggegevens met betrekking tot zijn epd³.

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.

Opvallend is dat, zolang nog geen voorzieningen zijn getroffen voor elektronische toegang door de patiënt (art. 13a lid 2), inzage in het epd uitsluitend via de zorgverlener verloopt (art. 13e lid 3). Het "klantenloket" is hierbij volgens het wetsvoorstel niet behulpzaam (art. 13i). Gezien de opzet van het EPD (zie hierboven onder 1.2.) is dit voor de patiënt die alle hem betreffende gegevens in het EPD wil inzien onnodig bezwarend en is hier juist wel een rol voor het klantenloket weggelegd. De bedoeling van het klantenloket is immers dat de patiënt niet van het kastje naar de muur wordt gestuurd.

³ *epd* (in kleine letters) wordt in dit advies gebruikt voor een individueel elektronisch dossier; dit in tegenstelling tot *EPD* (hoofdletters), dat gebruikt wordt in de context van het systeem.

In het wetsvoorstel ontbreekt de plicht tot *actieve* informatieverschaffing aan patiënten over het gebruik van zijn EPD. Het verdient aanbeveling te regelen dat patiënten regelmatig – bijvoorbeeld 1 of 2x per jaar - actief worden geïnformeerd over wie toegang heeft gehad tot zijn EPD.

2.5.3.2. Bezwaar tegen verwerking; verwijdering en afscherming van gegevens

De artikelen 13a lid 2 sub c, 13c lid 2, 13e lid 2 en 5 en 13i lid 1 sub b onder 2 hebben betrekking op de mogelijkheden van de patiënt om verwerking van zijn epd-gegevens te voorkomen of stop te zetten (opt-out).

Het gaat dan om het geheel of gedeeltelijk afschermen van de indexgegevens (art. 13a lid 2 sub c), het geheel of gedeeltelijk afschermen *of vernietigen* van de indexgegevens (art. 13c lid 2, art. 13i lid 1 sub b onder 2), bezwaar tegen (bepaalde) verwerkingen van indexgegevens, *persoonsgegevens betreffende de gezondheid van de patiënt en patiëntgegevens* (art. 13e lid 2) en het geheel of gedeeltelijk afschermen van de *epd-gegevens* (art. 13e lid 5).

Gezien het uitgangspunt dat niemand kan worden verplicht om aan het EPD deel te nemen, moet in het juridische kader worden voorzien in heldere procedures voor volledige en gedeeltelijke terugtrekking uit een EPD-systeem. In het wetsvoorstel is niet voldoende duidelijk geregeld hoe, waar en onder welke voorwaarden een burger zich kan “uitschrijven” uit het EPD en welke – al dan niet onomkeerbare – gevolgen dit heeft.

De opt-out mogelijkheden zijn geregeld in vier verspreide bepalingen, met deels overeenkomende, deels verschillende regimes en terminologie. Hierdoor rijzen vele vragen:

- waarom is “vernietigen” van de indexgegevens wel mogelijk in art. 13c lid 2 en niet in art. 13a lid 2 sub c?
- in hoeverre wijken de gevolgen van “vernietigen” van de indexgegevens af van “afschermen” van de indexgegevens?
- geldt het “bezwaar” in art. 13e lid 2 voor alle verwerkingen van art. 13d lid 1 sub b tot en met e tezamen, of wordt bedoeld bezwaar mogelijk te maken per individuele verwerking?
- wat zijn de verschillen in het gevolg van a) afschermen van de indexgegevens, b) vernietigen van de indexgegevens, c) bezwaar als bedoeld in art. 13e lid 2, d) het geheel of gedeeltelijk afschermen van de gegevens als bedoeld in art. 13e lid 5?
- sluiten deze opt-out varianten elkaar uit of zullen zij gecombineerd voorkomen?

Het CBP voorziet een welhaast babylonische spraakverwarring, terwijl juist op dit punt maatschappelijke discussie valt te verwachten en rechtszekerheid dient te worden geboden. Het CBP adviseert het gehele opt-out regime te concentreren in één wettelijke bepaling, die zo weinig mogelijk ruimte laat voor misverstanden. Daarbij dient rekening te worden gehouden met art. 7:455 lid 1 BW.

2.5.3.3. Overig

De strekking van art. 13i lid 1 sub c tenslotte is niet helder. Met name is niet duidelijk wat bedoeld wordt met het “herstellen (...) van verwerkingen van persoonsgegevens”. Ook zijn kennelijk gevallen voorzien waarin strijd met een wettelijk voorschrift niet kan worden vastgesteld maar slechts wordt vermoed, met toch als gevolg dat een verwerking wordt “hersteld” of “beëindigd”. Het CBP kan ook hiervan de consequenties niet overzien en adviseert deze bepaling te verhelderen.

2.5.4. Toezicht

Het CBP ziet in Nederland toe op de verwerking van persoonsgegevens (art. 51 lid 1 WBP). Daarnaast houdt IGZ toezicht op de gegevensverwerkingen bij de zorgverleners voor zover er een relatie is met de kwaliteit van de zorgverlening. CBP en IGZ hebben recent een samenwerkingsprotocol getekend, zodat zij bij samenlopende bevoegdheden de uitoefening van het toezicht op gegevensverwerkingen in de zorg coördineren (Staatscourant 2006, 233, p. 26).

Gegevensverwerkingen in het kader van het EPD kennen echter ook aspecten die geen relatie hebben met de kwaliteit van de zorg. In zulke situaties is IGZ niet bevoegd.

Gezien de omvang, complexiteit en risico's van het EPD kan waarschijnlijk niet met "algemeen" toezicht worden volstaan. Het staat buiten twijfel dat specifiek toezicht een forse inspanning van de toezichthouder vergt: de invoering van het EPD vergt extra toezichtscapaciteit die thans niet beschikbaar is.

Gezien het bovenstaande pleit het CBP voor specifiek toezicht, op te zetten vanuit de huidige toezichthouders CBP en IGZ met inachtneming van het thans geldende toezichtsarrangement, waar nodig aangevuld met aanvullende afspraken en bevoegdheden. Voor dit specifiek toezicht zullen extra middelen onontbeerlijk zijn.

2.5.5. Overig

2.5.5.1. Delegatie

Een punt van zorg is verder dat het wetsvoorstel veel delegatiebepalingen bevat:

- De regeling van bestuur en beheer van het LSP is gedelegeerd (art. 13a lid 3 en 4).
- Art. 13g delegeert de beschrijving van de successievelijke "hoofdstukken" van het EPD.
- Art. 17b delegeert regelgeving inzake de invoering van het EPD.
- Regels ten aanzien van beveiliging bij LSP zijn gedelegeerd (art. 13a lid 3).
- Regels m.b.t. "toezicht" op het LSP zijn gedelegeerd (art. 13a lid 3 en lid 4).

Het CBP wijst erop dat "bij wet bepaald" in art. 23 lid 1 sub e Wbp inhoudt dat regeling bij wet in formele zin is vereist. De verwerking van bijzondere persoonsgegevens dient dus in elk geval een grondslag te hebben in een wet in formele zin. Een wettelijke bepaling op grond van artikel 23 Wbp dient – mede gelet op artikel 8 EVRM en artikel 10 Grondwet – *voldoende specifieke* zijn. Bij besluit of ministeriële regeling mag slechts de *uitvoering* van de bepaling nader worden geregeld.

Het CBP adviseert om expliciet na te gaan of de bovenbedoelde delegaties voldoen aan deze uitgangspunten. Onder verwijzing naar de paragrafen 2.5.1. en 2.5.2.3. zij opgemerkt dat met name de delegaties in art. 13a lid 3 en 4 resp. art. 13a lid 3 wellicht ruimer zijn dan aanvaardbaar moet worden geacht.

Het CBP erkent overigens dat delegatie soms onontkoombaar is. Dit geldt bijvoorbeeld voor art. 13g. Een van de moeilijkste vragen bij de invoering van een EPD-systeem is immers de beslissing welke categorieën medische gegevens in het EPD moeten worden ingevoerd, en hoe lang ze moeten worden bewaard. Deze vraag moet in de eerste plaats worden beantwoord door medische experts, maar heeft ook aspecten die met gegevensbescherming samenhangen: artikel 11 lid 1 Wbp vereist dat verwerking van persoonsgegevens wordt beperkt tot gegevens die ter zake dienend en niet bovenmatig zijn voor de doeleinden waarvoor zij worden verwerkt.

Bijzondere aandacht verdient nog art. 17 lid 4 jo. lid 1. Naar het CBP uit de MvT begrijpt biedt dit artikellid een experimenteergrondslag voor delegatie waarbij in de lagere regeling kan worden afgeweken van de hogere. De Aanwijzing voor de regelgeving 10a vergt dat in een dergelijk geval in de hogere regeling is bepaald op welke onderdelen de mogelijkheid tot afwijking betrekking heeft. Art. 17 kent zo'n begrenzing niet. Daarnaast kan volgens de Aanwijzing afwijking slechts plaats vinden bij algemene maatregel van bestuur, en niet "bij of krachtens de algemene maatregelen van bestuur" zoals art. 17 lid 1 voorschrijft.

Bij de beoordeling van de toelaatbaarheid van deze delegatiebepaling dient voorts acht te worden geslagen op de op 22 mei 2007 door de Eerste Kamer aangenomen motie-Jurgens en de brief van 11 mei 2007 van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie⁴.

Op grond van artikel 51 lid 2 Wbp dient het CBP om advies te worden gevraagd over de bij dit wetsvoorstel gedelegeerde regelgeving. Gezien de grote impact van het EPD op de bescherming van persoonsgegevens enerzijds en de omvang van de delegatie anderzijds, geldt dit in dit geval bij wijze van waarborg ex artikel 23 lid 1 sub e Wbp ook voor de ministeriële regelingen.

2.5.5.2. Aansprakelijkheid

Een EPD-systeem moet ook garanderen dat mogelijke inbreuken op de persoonlijke levenssfeer als gevolg van de opslag en de verstrekking van medische gegevens in een dergelijk systeem in voldoende mate worden gecompenseerd door aansprakelijkheid voor schade door bijvoorbeeld onjuist of onbevoegd gebruik van EPD-gegevens.

Er dient een grondig civiel- en gezondheidsrechtelijk onderzoek te worden uitgevoerd om duidelijkheid te krijgen over nieuwe aansprakelijkheidsvraagstukken die zich in dit verband kunnen voordoen. Het gaat hier bijvoorbeeld om de nauwkeurigheid en volledigheid van de in het EPD ingevoerde gegevens, de vaststelling in welke mate de zorgverlener bij de behandeling van een patiënt het EPD moet bestuderen en de aansprakelijkheidsrechtelijke consequenties indien het EPD op zeker moment om technische redenen niet toegankelijk zou zijn voor de zorgverlener.

⁴ Kamerstukken I 2006/07, 26.200 VI, nr. 65; 21.109, D