CBPL
Commissie voor de bescherming van de persoonlijke levenssfeer

e health

Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid
Afdeling « Gezondheid»

SCSZG/14/114

BERAADSLAGING NR. 14/059 VAN 15 JULI 2014 MET BETREKKING TOT DE MEDEDELING VAN GECODEERDE PERSOONSGEGEVENS DIE DE GEZONDHEID BETREFFEN IN HET KADER VAN HET THALES PROJECT

De afdeling gezondheid van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid (hierna "het Sectoraal Comité" genoemd),

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens;*

Gelet op de machtigingsaanvraag van Cegedim en de bijkomende informatie;

Gelet op het auditoraatsrapport van het eHealth-platform van 11 juni 2014;

Gelet op het verslag van de heer Yves Roger;

Beslist op 15 juli 2014, na beraadslaging, als volgt:

I. ONDERWERP VAN DE AANVRAAG

1. Cegedim Strategic Data Belgium nv (CSD), filiaal van Cegedim France, verzoekt de goedkeuring van het Sectoraal comité voor de mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen door zorgverleners in het kader van het Thales project.

2. Het Thales project beoogt de verwezenlijking van wetenschappelijk statistische studies gebaseerd op longitudinale analyses van pathologieën, patiënt-profielen, therapeutische schema's teneinde een nieuwe en actuele kijk te krijgen op bepaalde medische en socio-economische gezondheidsproblemen en een diepere kennis te verwerven over de epidemiologische evolutie van bepaalde pathologieën. De resultaten van de analyses worden door CSD op de markt aangeboden aan farmaceutische bedrijven, diverse autoriteiten en de academische wereld.

3. De realisatie van dit project vereist de mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen bij een constant panel van 300 huisartsen uitgerust met de EMD software Health One[1]. De patiënten worden over de gegevensverwerking geïnformeerd en krijgen de mogelijkheid om zich tegen de verwerking te verzetten.

4. Volgende gegevens worden op continue wijze ingezameld per patiënt:

- patiëntgegevens: de (dubbel te coderen, cfr. infra) patiëntidentificatie (initieel toegekend door de Health One software), de provincie, één van dertien beroepsklassen, burgerlijke staat, aantal kinderen
- gecodeerde artsidentificatie
- antecedenten (vroegere pathologieën, pathologieën in de familie)
- allergieën (type, startdatum)
- gegevens betreffende de consultaties (reden, typische parameters zoals gewicht, bloeddruk)
- voorschriften
- chronische behandeling
- doorverwijzingen naar een specialist
- vaccinatie
- paramedische behandelingen
- onderzoeken

5. De gegevensstroom verloopt als volgt:

a) de arts exporteert de gegevens van patiënten die deelnemen aan de studie
   - de arts heeft de mogelijkheid tot verificatie van de gegevens voor verzending
   - lokaal bij de arts wordt de patiëntidentificatie een eerste maal gecodeerd

b) de gegevens worden door de huisartsensoftware verstuurd naar Custodix (dat optreedt als intermediaire organisatie) over een geauthentiseerd en geëncrypteerd communicatiekanaal
   - de data worden gefilterd op zeldzame pathologieën die tot indirecte heridentificatie zouden kunnen leiden

c) 2de codering bij Custodix
   - de gecodeerde patiëntidentificatie wordt een tweede maal gecodeerd
   - de artsidentificatie wordt een eerste maal gecodeerd
   - er wordt gecontroleerd of de data enkel de vastgelegde lijst van gegevens bevatten
   - controle op data filtering wordt doorgevoerd op niveau van de intermediaire organisatie

d) Cegedim France ontvangt de gecodeerde persoonsgegevens
   - de gecodeerde persoonsgegevens worden veilig opgeslagen voor verdere wetenschappelijke statistische verwerking
   - na dertig jaar worden de gegevens gewist

6. Custodix heeft geen toegang tot de eigenlijke patiëntidentificaties. Het ontvangt uitsluitend irreversibel gecodeerde patiënt pseudoniemen. De ontvangende partij Cegedim heeft noch toegang tot patiëntidenficatoren, noch tot de dokteridentificatoren.

[1] De softwareproducent in kwestie is HDMP (Health One Data Management Partners). De software Health One werd in 2014 geregistreerd in het kader van de telematica-premie. Cfr. https://www.ehealth.fgov.be/nl/ehealth-de-praktijk/registratie-van-de-medische-softwarepakketten

II. BEVOEGDHEID

7. Overeenkomstig artikel 42, § 2, 3°, van de wet van 13 december 2006 houdende diverse bepalingen betreffende gezondheid vereist iedere mededeling van persoonsgegevens die de gezondheid betreffen, behoudens de voorziene uitzonderingen, een principiële machtiging van het Sectoraal comité.

8. Gelet op het voorgaande is de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid van oordeel dat zij zich kan uitspreken over de mededeling van persoonsgegevens die de gezondheid betreffen zoals beschreven in de machtigingsaanvraag.

III. ALGEMEEN: DE VEREISTEN WAARAAN IEDERE TRUSTED THIRD PARTY DIE GEGEVENS CODEERT, MOET VOLDOEN

9. Het Sectoraal comité wijst er op dat de Commissie voor de bescherming van de persoonlijke levenssfeer in de aanbeveling nr. 02/2011 van 4 mei 2011 een aantal voorwaarden heeft geformuleerd voor de realisatie van onderzoeken gebaseerd op gezondheidsgegevens die afkomstig zijn uit een informaticaprogramma dat aan een geneesheer ter beschikking werd gesteld. Bovendien werd in de aanbeveling nr. 02/2010 van 31 maart 2010 de privacybeschermende rol van Trusted Third Parties bij gegevensuitwisseling verduidelijkt, waarbij de Commissie heeft geadviseerd over de te respecteren principes.

10. Rekening houdend met voormelde aanbevelingen, acht het Sectoraal comité het aangewezen om op algemene wijze de functionele vereisten te formuleren waaraan iedere Trusted Third Party (TTP) die persoonsgegevens codeert[2] effectief moet voldoen:

- De TTP dient voldoende onafhankelijk te zijn ten overstaan van zowel de verzender(s) van de te coderen persoonsgegevens als van de ontvanger(s) van de gecodeerde persoonsgegevens.

  De TTP-functie dient te worden uitgeoefend door een organisatie die op geen enkele wijze gelieerd is aan de verzender(s) van de niet-gecodeerde persoonsgegevens en aan de bestemmeling(en) van de gecodeerde persoonsgegevens.

  Indien de organisatie die als TTP optreedt toch op enigerlei wijze gelieerd is aan de verzender(s) of de bestemmeling(en), dienen de aanvrager en de TTP aan te tonen op welke wijze de vereiste onafhankelijkheid wordt gegarandeerd.

- De TTP dient de codering uit te voeren aan de hand van technieken die het redelijkerwijs niet mogelijk maken om de gecodeerde persoonsgegevens om te zetten in niet-gecodeerde persoonsgegevens. De codering dient in principe alle

[2] Behoudens specifieke situaties die door of krachtens de wet zijn geregeld, gelden deze vereisten zowel voor TTP's die optreden als intermediaire organisatie in de zin van hoofdstuk II van het koninklijk besluit van 13 februari 2001 als voor TTP's die tussenkomen voor de codering buiten de context van de latere verwerking van persoonsgegevens voor historische, statistische of wetenschappelijke doeleinden.

geïdentificeerde of identificeerbare personen te betreffen, zowel de personen op wie de persoonsgegevens die de gezondheid betreffen van toepassing zijn (bv. patiënten) als op de personen die de gegevens zouden verstrekken (bv. zorgverleners).

De TTP dient technisch en functioneel te beschrijven op welke wijze de codering zal worden uitgevoerd.

De TTP moet minstens volgende garanties bieden:

- De codering van de persoonsgegevens dient te worden uitgevoerd door het verwijderen van alle persoonsgegevens die tot een rechtstreekse identificatie kunnen leiden (zoals naam, voornaam, adres, enz.) en door de codering van een uniek identificatienummer per betrokkene.
- De codering van het identificatienummer dient te gebeuren door het omzetten van het identificatienummer in een gecodeerd nummer door middel van een conversietabel of door middel van een codeersleutel met een voldoende lange sleutellengte overeenkomstig de vigerende veiligheidsnormen.
- De TTP moet voor ieder project een specifieke, unieke codering toepassen die, behoudens specifieke machtiging van het Sectoraal comité, voor geen enkel andere codeeropdracht mag worden gebruikt.
- De mededeling van elk bericht met persoonsgegevens in het kader van de TTP-opdracht aan of door de TTP dient te worden versleuteld zodat uitsluitend de bestemmeling in kwestie (de TTP dan wel de ontvanger van de gecodeerde gegevens) het bericht kan ontcijferen.
- Voor zover de berichten meegedeeld aan de TTP persoonsgegevens bevatten die niet noodzakelijk zijn voor het uitvoeren van de TTP-opdrachten (codering of small cell risk analyse), dienen deze persoonsgegevens door de verzender te worden versleuteld, zodat uitsluitend de bestemmeling van de gecodeerde persoonsgegevens deze kan ontcijferen.
- De codeersleutel of conversietabel mag slechts bewaard worden gedurende de looptijd van de codeeropdracht, overeenkomstig de modaliteiten van de machtiging van het Sectoraal comité.

Indien de wijze van codering afwijkt van deze modaliteiten, moet de TTP aantonen dat een evenwaardig niveau van veiligheid wordt gegarandeerd.

- De TTP dient er – met kennis van zaken – voor te zorgen dat aan de hand van de ter beschikking gestelde set van gecodeerde persoonsgegevens redelijkerwijs geen mogelijkheid tot heridentificatie is (de zogenaamde small cells risk). Dit betekent dat er in voorkomend geval binnen de TTP specifieke competenties vereist zijn om de mogelijkheid tot heridentificatie aan de hand van gecodeerde persoonsgegevens die de gezondheid betreffen, te kunnen beoordelen.

  De TTP moet een technische en functionele beschrijving geven van de wijze waarop de small cell risk analyse wordt uitgevoerd en in welke bewerkingen er wordt voorzien om de heridentificatie aan de hand van de ter beschikking gestelde set van gecodeerde persoonsgegevens te voorkomen.

  De TTP moet aantonen dat de specifieke competenties voor de concrete opdracht aanwezig zijn.

- De verwerking van persoonsgegevens die de gezondheid betreffen door een TTP dient te gebeuren onder het toezicht en de verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg, bij voorkeur een geneesheer.

  De identiteit en de voor de opdracht relevante kwalificaties van de betrokken geneesheer moeten worden meegedeeld. Indien het geen geneesheer betreft, moet de TTP aantonen dat de voorgestelde beoefenaar van een gezondheidszorgberoep een evenwaardige garantie biedt.

- De TTP dient, al dan niet intern, een consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer aan te wijzen.

  De TTP moet de identiteit van de voorziene consulent inzake informatieveiligheid meedelen en aantonen dat deze over de voor de opdracht vereiste kwalificaties beschikt.

- De TTP moet waken over de correcte naleving van de wetgeving inzake de persoonlijke levenssfeer en moet alle nodige handelingen stellen om de naleving ervan te verzekeren.

  De TTP dient op erewoord te verklaren dat aan deze verplichting wordt voldaan.

- De TTP mag de gegevens die hij heeft verwerkt in het kader van zijn TTP-functie niet voor andere doeleinden gebruiken dan de specifieke doelen waarmee hij werd belast.

  De TTP dient op erewoord te verklaren dat aan deze verplichting wordt voldaan.

- De TTP moet de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere ander niet toegelaten verwerking van persoonsgegevens.

  De TTP en de aanvrager dienen op erewoord te verklaren dat aan deze verplichting wordt voldaan.

- De TTP moet alle gegevens vernietigen die hem door de verantwoordelijken van de oorspronkelijke verwerking werden bezorgd zodra hij zijn coderingsopdracht heeft vervuld.

- Enkel indien strikt noodzakelijk en mits machtiging van het Sectoraal comité mag de TTP het verband tussen het identificatienummer en het gecodeerd nummer bewaren (bv. voor longitudinale studies).

  In dit geval dient de TTP aan te tonen dat hij de vereiste gepaste technische en organisatorische maatregelen treft overeenkomstig de referentiemaatregelen die door de Commissie voor de bescherming van de persoonlijke levenssfeer werden opgesteld.

- De verwerkingen die door een TTP worden uitgevoerd, moeten transparant verlopen. Dit impliceert dat:
  - de verantwoordelijke van de oorspronkelijke en/of van de latere verwerking, vanwege de TTP minstens informatie krijgt over de werking, de voorwaarden voor het gebruik van de diensten en de draagwijdte van de aansprakelijkheid van de TTP;
  - de betrokkenen – op basis van de door de TTP en de verantwoordelijken voor de oorspronkelijke en/of latere verwerking verstrekte informatie – steeds moeten kunnen weten bij wie zij hun recht van toegang, verbetering, verwijdering of niet-aanwending kunnen uitoefenen;

  De TTP en de aanvrager dienen op erewoord te verklaren dat aan deze verplichting wordt voldaan.

IV. BEHANDELING VAN DE AANVRAAG

A. FINALITEITSBEGINSEL

11. Krachtens artikel 4, § 1, 2°, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna genoemd: 'de privacywet') is de verwerking van persoonsgegevens enkel toegelaten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

12. Het Sectoraal comité stelt vast dat de beoogde gegevensverwerking tot doel heeft om wetenschappelijk en/of statistische studies en analyses uit te voeren overeenkomstig de principes zoals hoger uiteengezet. Het Sectoraal comité neemt akte van het feit dat de resultaten van de wetenschappelijk statistische studies zullen worden gecommercialiseerd en op de markt zullen worden aangeboden. De verwerking beantwoordt dan ook aan welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

13. De verwerking van persoonsgegevens betreffende de gezondheid is in principe verboden overeenkomstig artikel 7, § 1, van de privacywet. Overeenkomstig artikel 7, § 2, k), van deze wet geldt dit verbod evenwel niet wanneer de verwerking van persoonsgegevens die de gezondheid betreffen noodzakelijk is voor wetenschappelijk onderzoek en verricht wordt onder de voorwaarden vastgesteld door de Koning. De aanvrager is meer specifiek gehouden de verplichtingen van het koninklijk besluit van 13 februari 2001 tot uitvoering van de privacywet na te leven.

B. PROPORTIONALITEITSBEGINSEL

14. In artikel 4, § 1, 3° van de privacywet wordt bepaald dat de persoonsgegevens toereikend, terzake dienend en niet overmatig dienen te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt.

15. Rekening houdend dat de beoogde wetenschappelijke en/of statistische analyses longitudinale studies betreffen die dezelfde patiënten gedurende de loop ter tijd opvolgen. Het is bijgevolg noodzakelijk dat de verwerking wordt verricht met gecodeerde persoonsgegevens.

16. De resultaten van de analyses van de gecodeerde persoonsgegevens zullen worden gebruikt om het geneesmiddelengebruik te bepalen (bv. therapeutische schema's volgens indicatie, compliancedoeleinden – gebruik buiten indicatie, …), om outcome research studies en gezondheidseconomische evaluaties te realiseren en om het natuurlijke verloop van een pathologie te kunnen inschatten. De incidentie en prevalentie van ziekten alsook de patiëntenprofielen vormen een belangrijke informatiebron voor farmaceutische bedrijven en autoriteiten om market access dossiers te ondersteunen alsook een belangrijke bron voor de academische wereld in het kader van onderzoeksprojecten.

17. Het Thales project beoogt enkel statistische studies onder volgende voorwaarden:

- resultaten worden standaard aangeleverd op Belgisch niveau (aggregatie): nooit op individueel niveau en het laatst mogelijke niveau van granulatie is een onderscheid tussen Vlaanderen, Wallonië en Brussel
- resultaten worden geëxtrapoleerd naar het universum: er worden geen delen van de databank doorgegeven, het bevat geen gegevens op individuele lijnen
- het betreft statistisch betrouwbare resultaten: geen analyses mogelijk op pathologieën waarvoor incidentie te klein is (de weesziekten worden uitgesloten uit de databank) en geen segmenteringen waarvoor te weinig volume aanwezig is.

18. Volgende analyses worden aan de hand van de Thales gegevens uitgevoerd:

- epidemiologische studies: prevalentie, incidentie, comorbiditeiten, risicofactoren, evolutie (longitudinale analyse), behandeld/onbehandeld
- geneesmiddelengebruik: therapeutisch behandelgingsschema, dynamiek van de markt (verandering behandelingsschema doorheen de tijd), patiënten profielen/-segmenten (leeftijd, geslacht, BMI, abdominale perimeter, roken, alcohol), klinisch profiel (klinische events, diagnoses, indicaties, symptomen, labo resultaten, comorbiditeiten, risicofactoren, verwijzing specialist), voorschriften – marktgrootte (data Rx, ATC, molecule, dosering, duurtijd behandeling, behandelingsschema, Rx evolutie), compliance: gebruik geneesmiddelen per indicatie, disease management strategieën.

19. Rekening houdend met het voorgaande, acht het Sectoraal comité de persoonsgegevens toereikend, terzake dienend en niet overmatig.

20. Overeenkomstig artikel 4, § 1, 5°, van de privacywet mogen persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verkregen of verder worden verwerkt. De aanvrager voorziet er in dat de gecodeerde persoonsgegevens worden bewaard voor een periode van 30 jaar. Gelet op het longitudinaal karakter van de beoogde analyses kan deze bewaartermijn worden aanvaard.

C. TRANSPARANTIEBEGINSEL

21. Overeenkomstig artikel 9 van de privacywet moet de verantwoordelijke voor de verwerking bepaalde informatie verstrekken aan de betrokkene.

22. Het Sectoraal comité stelt vast dat de betrokkenen worden geïnformeerd door een poster in de wachtkamer van de betrokken artsen, door de terbeschikkingstelling van brochures en door de betrokken artsen zelf. Het Sectoraal comité acht het evenwel

aangewezen dat in de informatieverstrekking eveneens uitdrukkelijk wordt verwezen naar de huidige beraadslaging.

23. Teneinde de betrokken patiënten voldoende bedenktijd te geven, is het Sectoraal comité van oordeel dat deze over een periode van zeven kalenderdagen moeten kunnen beschikken om hun eventuele weigering mee te delen aan hun huisarts.

D. VEILIGHEIDSMAATREGELEN

24. Overeenkomstig artikel 7, § 4 van de privacywet mogen persoonsgegevens betreffende de gezondheid enkel worden verwerkt onder het toezicht en de verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg. Hoewel dit strikt genomen niet wordt vereist in de privacywet, verdient het volgens het Sectoraal Comité de voorkeur dat dergelijke gegevens worden verwerkt onder de verantwoordelijkheid van een geneesheer[3], hetgeen in casu het geval is. Het Comité herinnert er bovendien aan dat de beroepsbeoefenaar in de gezondheidszorg en zijn aangestelden of gemachtigden bij de verwerking van persoonsgegevens tot geheimhouding verplicht zijn.

25. Overeenkomstig artikel 16, § 4, van de privacywet moet de aanvrager verder alle gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de bescherming van de persoonsgegevens. Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.

26. Om de vertrouwelijkheid en de veiligheid van de gegevensverwerking te garanderen, moet iedere instelling die persoonsgegevens bewaart, verwerkt of meedeelt maatregelen nemen in de volgende elf actiedomeinen die betrekking hebben op de informatieveiligheid: veiligheidsbeleid; aanstelling van een informatieveiligheidsconsulent; organisatorische en menselijke aspecten van de veiligheid (vertrouwelijkheidsverbintenis van het personeel, regelmatige informatieverstrekking en opleidingen ten behoeve van het personeel inzake bescherming van de privacy en veiligheidsregels); fysieke veiligheid en veiligheid van de omgeving; netwerkbeveiliging; logische toegangs- en netwerkbeveiliging; loggings, opsporing en analyse van de toegangen; toezicht, nazicht en onderhoud; systeem van beheer van de veiligheidsincidenten en de continuïteit (backup-systemen, fault tolerance-systemen, …); naleving en documentatie. Het Sectoraal comité mocht de Information System Security Policy van Cegedim ontvangen waaruit moet blijken dat er wordt voldaan aan de vereisten op het vlak van vertrouwelijkheid en veiligheid. Het Sectoraal comité ontving eveneens de Security Practice Statement evenals de Information Governance Policy van Custodix waaruit moet blijken dat er wordt voldaan aan de vereisten op het vlak vertrouwelijkheid en veiligheid. Het Sectoraal comité neemt akte van het feit dat beide instellingen een informatieveiligheidsconsulent hebben aangeduid en dat de verwerking van de gezondheidsgegevens onder de verantwoordelijkheid van een geneesheer verloopt.

27. Wat de rol van de intermediaire organisatie betreft, heeft de Commissie voor de bescherming van de persoonlijke levenssfeer bevestigd dat de betreffende instelling

[3] Het Sectoraal Comité heeft deze voorkeur opgesteld in zijn beraadslaging nr. 07/034 van 4 september 2007 met betrekking tot de mededeling van persoonsgegevens aan het Federaal Kenniscentrum voor de Gezondheidszorg met het oog op het onderzoek 2007-16-HSR “Onderzoek naar mogelijke financieringsmechanismen voor het geriatrisch dagziekenhuis”.

onafhankelijk moet zijn van zowel de initiële verantwoordelijke voor de verwerking (in casu de huisartsen) als van de ontvangers van de persoonsgegevens die ze zullen verwerken voor statistische of wetenschappelijke doeleinden. Dergelijke instelling mag dus voor dergelijke onderzoeksdoeleinden, de inhoud niet zelf onderzoeken of analyseren. De intermediaire instelling mag een concordantietabel bijhouden die het verband bevat tussen de ter beschikking gestelde, gecodeerde persoonsgegevens enerzijds en de identiteit van de personen waarop ze betrekking hebben anderzijds, zodat ze later nieuwe gecodeerde persoonsgegevens of bijkomende gegevens over diezelfde personen kan leveren. Buiten de identificeerbare gegevens uit de concordantietabel die gecodeerd mogen worden, dient de intermediaire organisatie geen persoonsgegevens te bewaren.[4] In casu wordt er in voorzien dat de intermediaire organisatie reeds voor een eerste maal gecodeerde persoonsgegevens ontvangt en ze een tweede maal codeert alvorens aan de ontvangers mee te delen. De intermediaire organisatie verwijdert alle persoonsgegevens na transmissie aan de ontvanger. Het Sectoraal comité stelt bijgevolg vast dat de voorgestelde werkwijze van intermediaire organisatie aan de gestelde voorwaarden voldoet.

28. Het Sectoraal Comité herinnert eraan dat het overeenkomstig artikel 6 van het koninklijk besluit van 13 februari 2001 *ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* verboden is om handelingen te stellen die ertoe strekken de gecodeerde persoonsgegevens om te zetten in niet-gecodeerde persoonsgegevens. Het niet-naleven van dit verbod kan, krachtens artikel 39, 1° van de privacywet, een geldboete tot gevolg kan hebben. Het Sectoraal Comité herinnert er ook aan dat bij een veroordeling wegens een misdrijf omschreven in artikel 39, de rechter de verbeurdverklaring kan uitspreken van de dragers van persoonsgegevens waarop het misdrijf betrekking heeft (zoals manuele bestanden, magneetschijven of magneetbanden) of de uitwissing van die gegevens kan gelasten. De rechter kan ook het verbod uitspreken om gedurende ten hoogste twee jaar rechtstreeks of door een tussenpersoon het beheer te hebben over enige verwerking van persoonsgegevens [5].

[4] Randnummer 24 van de aanbeveling nr. 02/2011 van 4 mei 2011.
[5] Artikel 41 van de privacywet.

Om deze redenen,

verleent de afdeling gezondheid van het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid

overeenkomstig de modaliteiten zoals beschreven in deze beraadslaging, een machtiging voor de mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen door huisartsen aan Cegedim in het kader van het Thales project, voor zover:

- de TTP die de persoonsgegevens codeert, voldoet aan de voorwaarden die worden opgelegd in randnummer 10 van deze beraadslaging;

- in de informatieverstrekking aan de betrokkenen uitdrukkelijk wordt verwezen naar deze beraadslaging;

- er in wordt voorzien dat de betrokkenen een bedenktijd van zeven kalenderdagen hebben om hun eventuele weigering mee te delen aan hun respectieve huisartsen.

Het Sectoraal comité bepaalt bovendien ten algemene titel dat iedere verantwoordelijke voor de verwerking moet garanderen dat wordt voldaan aan de vereisten zoals beschreven in randnummer 10 van deze beraadslaging indien bij de verwerking van persoonsgegevens die de gezondheid betreffen een TTP tussenkomt voor de codering

Yves ROGER
Voorzitter