Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid
Afdeling "Gezondheid"

SCSZG/14/173

BERAADSLAGING NR. 14/094 VAN 18 NOVEMBER 2014 BETREFFENDE DE MEDEDELING VAN GECODEERDE PERSOONSGEGEVENS DIE DE GEZONDHEID BETREFFEN DOOR WACHTPOSTEN AAN HET CENTRUM VOOR HUISARTSENGENEESKUNDE VAN DE UNIVERSITEIT ANTWERPEN IN HET KADER VAN HET ICAREDATA-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 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*;

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

Gelet op de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform*;

Gelet op de definitieve machtigingsaanvraag ontvangen op 13 oktober 2014;

Gelet op het auditoraatsrapport van het eHealth-platform van 7 november 2014;

Gelet op het verslag van de heer Yves Roger.

Beslist op 18 november 2014, na beraadslaging, als volgt:

I. ONDERWERP VAN DE AANVRAAG

1. Het Centrum voor Huisartsengeneeskunde, Vakgroep Eerstelijns- en Interdisciplinaire Zorg van de Faculteit Geneeskunde en Gezondheidswetenschappen van de Universiteit Antwerpen (CHA-ELIZA) legt het Sectoraal comité ter goedkeuring de mededeling van gecodeerde persoonsgegevens door wachtposten voor in het kader van de oprichting van een klinische research gegevensdatabank, *Improve Care and Research Electronic Data Trust Antwerp* (iCAREdata) genaamd.

2. Het doel van het project is om onderzoek naar de zorg buiten de normale werkuren (out-of-hours, OOH) mogelijk te maken en de kwaliteit van OOH-zorg te verbeteren. Momenteel mogen de gegevens van een patiëntencontact in een wachtpost niet langer dan 18 maanden worden bewaard, waardoor ze slechts voor een korte periode beschikbaar zijn voor onderzoek. Door het onderzoeksproject iCAREdata zal het mogelijk zijn om deze gegevens op gecodeerde wijze langduriger en daardoor diepgaander te kunnen onderzoeken. De gecodeerde persoonsgegevens worden geanalyseerd door onderzoekers van het CHA-ELIZA. Het onderzoek kan worden uitgevoerd op initiatief van CHA-ELIZA of op vraag van externe onderzoekers..

3. De benodigde persoonsgegevens worden op automatische wijze ingezameld bij de deelnemende wachtposten in het softwareprogramma van de wachtpost. De persoonsgegevens worden vervolgens via de eHealth-box overgemaakt aan het eHealth-platform dat als *trusted third party* (TTP) tussenkomt voor de codering van de identificatiegegevens van de patiënt en de betrokken zorgverleners, alvorens de gecodeerde persoonsgegevens worden meegedeeld aan het CHA-ELIZA. De patiënten worden geïnformeerd via een affiche in de wachtzaal en de arts kan tijdens de consultatie nadere informatie verstrekken. De patiënt heeft de mogelijkheid om deelname te weigeren en de huisarts kan de weigering registreren in het elektronisch medisch dossier.

4. Volgende gecodeerde persoonsgegevens die de gezondheid betreffen worden per betrokken patiënt meegedeeld:

<u>Patiëntgegevens</u>:
- het identificatienummer van de sociale zekerheid (INSZ) dat wordt gecodeerd door de TTP. Indien de patiënt geen INSZ bezit, wordt een nummer door de TTP toegekend.
- geboortejaar patiënt
- geslacht patiënt
- postcode woonplaats patiënt
- code verzekerbaarheid patiënt

Contactgegevens:
- identificatie contact,[1] gecodeerd door TTP
- identificatie wachtpost
- datum en tijdstip contact en start behandeling, wijze van contacteren, type contact, urgentieraad
- RIZIVnummer arts die contact behandeld, gecodeerd TTP
- Eventuele verwijzing, al dan niet arbeidsongeschiktheid

Morbiditeitsgegevens:
- Diagnose
    - Datum, contactreden (thesarusterm en code), diagnose (thesaurusterm en code)
    - Vrij tekstveld met subjectieve klachten patiënt
    - Vrij tekstveld met vaststellingen onderzoek
- Medicatievoorschriften
    - Datum, naam medicatie, CNK-code

5. Op de server of computer van de wachtpost wordt een comma separated value (csv) bestand aangemaakt. De eerste drie kolommen bevatten opeenvolgend het INSZ-nummer van de patiënt, het RIZIV-nummer van de arts en de identificatiecode van het contact. Deze drie kolommen worden gescheiden door een puntkomma van de volgende kolommen die de medische informatie bevatten. Deze kolommen met medische informatie worden voor verzending geëncrypteerd. Dit csv-bestand wordt beveiligd verzonden naar eHealth voor codering via de eHealthBox. Nadien worden de gecodeerde bestanden beveiligd verzonden naar de eHealthBox van iCAREdata.

6. In deze eHealthBox worden de eerste drie kolommen gecodeerd door eHealth. Dit gebeurt met een algoritme dat enkel gekend is door het eHealthplatform. Voor het RIZIV-nummer van de arts is dit een reversibel algoritme, voor het INSZ en identificatie van het contact is dit irreversibel. De geëncrypteerde velden met medische informatie, kunnen niet gelezen worden door het eHealthplatform aangezien het niet over de sleutel voor decryptie beschikt. Het bestand met gecodeerde identificatievelden en geëncrypteerde medische velden, wordt op regelmatige tijdstippen opgehaald door de server van de UA vanuit de eHealthBox.

7. Op de server van de UA worden door de onderzoekersploeg van iCAREdata de medische velden gedecrypteerd, de identificatievelden blijven gecodeerd. Met deze werkwijze kan het eHealth-platform geen medische gegevens lezen en kan de onderzoekersploeg van iCAREdata geen gegevens identificeren.

8. Teneinde de heridentificatie aan de hand van de combinatie van gecodeerde persoonsgegevens te vermijden, wordt een small cells risk analyse uitgevoerd in samenwerking met de Technische cel. Indien nodig zullen bepaalde gecodeerde persoonsgegevens worden geaggregeerd om te voorkomen dat de betrokkenen zouden kunnen worden geïdentificeerd.

[1] In het EMD van de wachtpost krijgt ieder contact met een patiënt een nummer toegewezen.

9. Voor het beheer van de iCAREdata-gegevensbank werden twee adviesraden opgericht: een wetenschappelijk comité en een stuurcomité. Het wetenschappelijk comité is samengesteld uit vertegenwoordigers van het CHA-ELIZA (artsen), vertegenwoordigers van de meewerkende wachtposten, een vertegenwoordiger van de UA-Herculusstichting en een patiëntenvertegenwoordiger. Het controleert de ontvankelijkheid en haalbaarheid van onderzoeksvragen en bewaakt de toepassing van de privacywetgeving. Het weert aanvragers met niet-wetenschappelijke, zuiver commerciële doelstellingen. Het controleert de kwaliteit van de verzamelde gegevens en de geleverde output door iCAREdata. Het stuurcomité is op zijn beurt samengesteld uit de supervisor, promotor, copromotor van het iCAREdata-project, de databeheerder (arts) en de betrokken CHA-leden, evenals een vertegenwoordiger van UA-Herculesstichting. De dataleveranciers kunnen actief of passief deelnemen aan de vergaderingen. Het is verantwoordelijk voor het management van iCAREdata (constructie en onderhoud van de infrastructuur), voor de opvolging van de werking van de infrastructuur (incl. website), beoordeling van de loggings, het financieel management, de feedback naar Herculesstichting, het onderhoud van contacten en het verzorging van de communicatie, de reactie op klachten en het behandelen van aanvragen tot opting-out (onderzoekers, artsen, patiënten, derden), de opvolging van het advies van het wetenschappelijk comité.

10. De gecodeerde persoonsgegevens van het iCAREdata-project worden wetenschappelijk geanalyseerd op initiatief van onderzoekers binnen het CHA-ELIZA en verbonden aan het iCAREdata-project dan wel op vraag van externe onderzoekers. De externe onderzoekers kunnen enkel de resultaten van de analyses (al dan niet in de vorm van aggregaties) ontvangen. Er worden géén gecodeerde persoonsgegevens meegedeeld aan externe onderzoekers zonder bijkomende machtiging van de afdeling gezondheid van het Sectoraal comité..

11. Onderzoekers die niet verbonden zijn aan het CHA-ELIZA, moeten een specifieke aanvraag indienen, waarna een overeenkomst wordt opgesteld met betrekking tot de gevraagde analyses. Deze overeenkomsten worden in beide adviesraden besproken.

12. Het RIZIV-nr. van de betrokken artsen wordt reversibel gecodeerd. Zodoende kan, via de tussenkomst van het eHealth-platform, tot decodering worden over gaan doch uitsluitend met betrekking tot het gecodeerd RIZIV-nr. van de geneesheren in kwestie teneinde de nodige feedback aan de betrokken geneesheer te kunnen verstrekken. Zo kan bijvoorbeeld aan een individuele arts meegedeeld worden, hoeveel en welke antibiotica hij voorschrijft bij een bepaalde infectie. De onderzoekers hebben op geen enkel ogenblik kennis van de identiteit van de betrokken geneesheren.

13. De gegevensbank van de iCAREdata-project wordt bewaard op een server die zich bevindt in een serverroom op Campus Middelheim van de Universiteit Antwerpen. Deze ruimte is fysiek enkel toegankelijk voor een beperkt aantal ICT medewerkers. De toegang tot de eigenlijke databank is beperkt tot de databeheerder (geneesheer) en een ICT-medewerker (bio-informaticus) van het iCAREdata-project. Ze hebben

enkel toegang via een beveiligde verbinding. Veiligheidsloggings betreffende de toegang tot de gegevensbank worden genomen.

II. BEVOEGDHEID

14. 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.

15. De mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen door wachtposten aan het CHA-ELIZA met het oog op de samenstelling van een register voor onderzoeksdoeleinden valt niet onder één van voormelde uitzonderingen, en vereist bijgevolg een machtiging van het Sectoraal comité.

III. BEHANDELING VAN DE AANVRAAG

A. FINALITEITSPRINCIPE

16. Krachtens artikel 4, § 1, van de privacywet mogen persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen en niet verder worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de redelijke verwachtingen van de betrokkene en met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden.

17. Het doeleinde van de gegevensverwerking is de samenstelling van een databank met gecodeerde gezondheidsgegevens om wetenschappelijk onderzoek mogelijk te maken. De Universiteit Antwerpen heeft als zelfstandige universiteit overeenkomstig haar statuten onder andere specifieke wetenschappelijke onderzoeksopdrachten te vervullen. Gelet op het voorgaande stelt het Sectoraal comité dan ook vast dat de beoogde verwerking een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde heeft.

18. Overeenkomstig de privacywet mogen persoonsgegevens niet verder worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name met de redelijke verwachtingen van de betrokkene en met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk werden verzameld. Het Sectoraal comité stelt vast dat in casu het doeleinde voor de latere verwerking slechts als verenigbaar kan worden beschouwd in zoverre de bepalingen van hoofdstuk II van het koninklijk besluit van 13 februari 2001 tot uitvoering van de privacywet worden nageleefd.

19. De verwerking van persoonsgegevens die de gezondheid betreffen is in principe verboden.[2] Dit verbod geldt echter niet, zoals in casu het geval is, wanneer de verwerking noodzakelijk is voor het wetenschappelijk onderzoek en verricht wordt onder de voorwaarden vastgesteld door de Koning.[3] De aanvrager is verplicht de bepalingen van het koninklijk besluit van 13 februari 2001 na te leven. De aanvrager is dan ook gehouden de verplichtingen zoals vermeld in artikelen 21 (met betrekking tot de uitbreiding van de verplichte aangifte), 23 (met betrekking tot de bekendmaking van de resultaten) en 25 (met betrekking tot de ter beschikking stelling van een lijst van categorieën van ontvangers) van voormeld koninklijk besluit na te leven.

B. PROPORTIONALITEITSPRINCIPE

20. 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.

21. Wat de verzamelde gecodeerde gezondheidsgegevens betreft, neemt het Sectoraal comité akte van het feit dat er slechts een beperkt aantal rechtstreeks identificerende persoonsgegevens worden verzameld, meer bepaald het geboortejaar, het geslacht, en de postcode van de woonplaats. Iedere patiënt wordt uniek geïdentificeerd aan de hand van een INSZ dat wordt gecodeerd door het eHealth-platform. De gezondheidsgegevens zelf beslaan de diagnose en het medicatiegebruik. Het Sectoraal comité stelt vast dat het beoogde klinisch onderzoek door het CHA-ELIZA wel degelijk specifieke informatie vereist over de incidentie en prevalentie van ziekten en medicatie, evenals gegevens over het contact met de wachtpost. De aanvrager stelt dat de beschreven gegevens toelaten dat uiteenlopende onderzoeksvragen betreffende de OOH-zorg kunnen worden behandeld. De meta-analyse van de gegevens kan een beter inzicht geven in de werking van de wachtposten.

22. Een latere verwerking van persoonsgegevens voor wetenschappelijke doeleinden dient in principe plaats te vinden aan de hand van anonieme gegevens. Indien het doeleinde niet kan worden verwezenlijkt met anonieme gegevens, mogen gecodeerde persoonsgegevens worden verwerkt. Gelet op het feit dat het noodzakelijk is dat een patiënt uniek wordt geïdentificeerd en het noodzakelijk is een patiënt te kunnen opvolgen in de tijd, is het aanvaardbaar dat met gecodeerde persoonsgegevens wordt gewerkt.

23. Wat de verwerking van de gecodeerde persoonsgegevens op vraag van externe onderzoekers betreft, stelt het Sectoraal comité vast dat de wetenschappelijke analyses die nodig zijn voor het beantwoorden van de onderzoeksvragen door de onderzoekers van het CHA-ELIZA verbonden aan het iCAREdata-project betreft

[2] Artikel 7, §1, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 18 maart 1993 (hierna 'privacywet' genoemd).
[3] Artikel 7, §2, k) van de privacywet.

zelf worden uitgevoerd. Iedere mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen uit de gegevensbank van het iCAREdata-project wordt voorafgaandelijk ter goedkeuring aan het Sectoraal comité voorgelegd.

24. Gelet op het voorgaande acht het Sectoraal comité de verwerking van de beoogde persoonsgegevens toereikend, terzake dienend en niet overmatig in het licht van de beoogde doeleinden.

25. Persoonsgegevens mogen in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verkregen of verder worden verwerkt, noodzakelijk is. De aanvrager voorziet in een bewaartermijn van 30 jaar vanaf de opname in de gegevensbank. Deze bewaartermijn moet toelaten om evoluties in de tijd te bestuderen. De aanvrager stelt dat de OOH-zorg een relatief recent fenomeen is en dat de werking een onvoorziene richting kan nemen. Ook trends in voorschrijfgedrag kunnen enkel na jaren worden bestudeerd. Het Sectoraal comité aanvaardt dan ook de voorgestelde bewaartermijn.

C. PRINCIPE VAN TRANSPARANTIE

26. De verantwoordelijke voor de verwerking van persoonsgegevens verzameld voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden of –in voorkomend geval– de intermediaire organisatie moeten in principe voorafgaand aan de codering van de persoonsgegevens aan de betrokken personen bepaalde informatie verstrekken omtrent de verwerking.

27. De aanvrager voorziet in een kennisgeving van de gegevensverwerking aan de betrokkene door middel van een affiche in de wachtzaal en de mogelijkheid van nadere informatieverstrekking door de huisarts tijdens de consultatie. Er wordt in de kennisgeving via de affiche eveneens verwezen naar voorliggende beraadslaging.

28. Het Sectoraal comité acht de voorziene kennisgeving voldoende.

D. VEILIGHEIDSMAATREGELEN

29. De verwerking van persoonsgegevens die de gezondheid betreffen moet gebeuren onder het toezicht en de verantwoordelijkheid van beroepsbeoefenaar in de gezondheidszorg[4]. Hoewel dit strikt genomen niet wordt vereist, verdient het volgens het sectoraal comité de voorkeur dat dergelijke gegevens worden verwerkt onder de verantwoordelijkheid van een geneesheer[5]. Het Sectoraal comité mocht effectief de identiteit van de betrokken geneesheer ontvangen. Het Sectoraal comité herinnert er aan dat de beroepsbeoefenaar in de gezondheidszorg en zijn

[4] Artikel 7, §4, van de privacywet.
[5] Beraadslaging nr. 07/034 van 4 september 2007.

aangestelden of gemachtigden bij de verwerking van persoonsgegevens tot geheimhouding verplicht zijn.

30. De verantwoordelijke voor de verwerking 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 andere niet toegelaten verwerking van persoonsgegevens[6]. Het Sectoraal comité verwijst hieromtrent naar de referentiemaatregelen die gelden voor de beveiliging van iedere verwerking van persoonsgegevens, opgesteld door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer.[7] 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.

31. Om de vertrouwelijkheid en de veiligheid van de gegevensverwerking te garanderen, moet iedere instelling die persoonsgegevens bewaart, verwerkt of meedeelt afhankelijk van de context en de aard van de persoonsgegevens 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 neemt akte van het feit dat de aanvrager bevestigt dat een informatieveiligheidsconsulent werd aangesteld. De lokalen waar de gecodeerde persoonsgegevens worden opgeslagen zijn beveiligd en zijn slechts toegankelijk voor daartoe gemachtigde personen. De toegang 'on-campus' via het netwerk tot de server is strikt geregeld en gebeurt op basis van IP adres en accountgegevens. De gebruikte protocollen worden, waar mogelijk, beveiligd door middel van SSL. Remote toegang tot de server is enkel mogelijk via SSL VPN-toegang en op grond van specifieke toegangsrechten. De toegang wordt eveneens gelogd. De server is voorzien van redundante onderdelen: dubbele voeding, RAID technologie, automatische monitoring van hardware en het nemen van backups.

32. Het Sectoraal comité wijst er volledigheidshalve op dat overeenkomstig artikel 6 van het koninklijk besluit van 13 februari 2001 het verboden is om handelingen te stellen die ertoe strekken de meegedeelde 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.

---

[6] Artikel 16 van de privacywet.

[7] http://www.privacycommission.be/nl/static/pdf/referentiemaatregelen.pdf

Het Sectoraal Comité herinnert eraan 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.

Om deze redenen, verleent

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

een machtiging betreffende de mededeling van gecodeerde persoonsgegevens die de gezondheid betreffen door wachtposten aan het Centrum voor Huisartsengeneeskunde van de Universiteit Antwerpen in het kader van het iCAREdata-project, met tussenkomst van het eHealth-platform voor de codering van de persoonsgegevens.

Het eHealth-platform wordt gemachtigd om het verband tussen het gecodeerde nummer en het reële identificatienummer te bewaren gelet op het longitudinaal karakter van het project. Bovendien wordt het eHealth-platform gemachtigd om tot decodering over te gaan doch uitsluitend met betrekking tot het gecodeerd RIZIV-nr. van de artsen in kwestie teneinde de nodige feedback aan de betrokken arts te kunnen verstrekken. Hierbij mogen nooit (al dan niet gecodeerde) persoonsgegevens betreffende de individuele patiënten worden meegedeeld.

Yves ROGER
Voorzitter