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

SCSZG/12/049

BERAADSLAGING NR 11/014 VAN 15 FEBRUARI 2011, LAATST GEWIJZIGD OP 20 MAART 2012, MET BETREKKING TOT DE MEDEDELING VAN PERSOONSGEGEVENS DIE DE GEZONDHEID BETREFFEN IN HET KADER VAN DE WEBTOEPASSING 'WEBWACHTMAILER'

De afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid (*hierna genoemd: "het Sectoraal comité*"),

Gelet op artikel 42, §2, 3°, van de wet van 13 december 2006 houdende diverse bepalingen betreffende de gezondheid;

Gelet op artikel 11 van de wet van 21 augustus 2008 tot oprichting en organisatie van het eHealth-platform;

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

Gelet op de beraadslaging van 15 februari 2011, gewijzigd op 22 november 2011, van het Sectoraal comité;

Gelet op het verzoek tot wijziging van voormelde beraadslaging, ontvangen op6 februari 2012;

Gelet op het auditoraatsrapport van het eHealth-platform van 12 maart 2012;

Gelet op het verslag van de heer Yves Roger,

Beslist op 20 maart 2012, na beraadslaging, als volgt:

I. VOORWERP VAN DE AANVRAAG

1. Hermes vzw stelt een webtoepassing ter beschikking waarmee een wachtarts een wachtverslag kan opstellen in het kader van de huisartsenwachtdienst. Deze webtoepassing heeft twee doeleinden:
   - door het opstellen en het overmaken van het wachtverslag door de wachtarts aan de huisarts van de betrokken patiënt kan de continuïteit van zorg worden verzekerd;
   - een selectie van gecodeerde persoonsgegevens afkomstig van deze wachtverslagen wordt meegedeeld aan de coördinator van iedere wachtkring voor de redactie van de wettelijk verplichte jaarlijkse rapportering aan de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu over de werking van de wachtdiensten waarin uitsluitend geanonimiseerde en geaggregeerde gegevens worden opgenomen.

2. Al naargelang de functie van receptionist op de wachtpost van de betrokken kring voorzien is, wordt een verschillende procedure voor het aanmaken van een wachtverslag gevolgd. Indien een receptionist aanwezig is, registreert deze eerst een beperkt aantal persoonsgegevens van de patiënt. Deze gegevens worden opgeslagen in een 'wachtkamerlijst'. Indien de wachtarts in kwestie vervolgens het wachtverslag opmaakt, worden de persoonsgegevens afkomstig van de wachtkamerlijst automatisch ingevuld in het wachtverslag, dat door de wachtarts wordt vervolledigd. Indien de functie van receptionist niet is voorzien, is er geen wachtkamerlijst en dient de betrokken wachtarts alle vereiste persoonsgegevens zelf in te vullen.

3. Indien de functie van receptionist op de wachtpost van de betrokken kring is voorzien, logt de receptionist in door middel van zijn eID[1]. Aan de hand van de gegevens van de eID identificeert en authenticeert het gebruikers- en toegangsbeheer van het eHealth-platform de betrokken persoon en geeft het de identificatiegegevens van de betrokkene door aan de 'Access Control List' van de webtoepassing. Deze Access Control List bevat de toegangsrechten van de gebruikers van de webtoepassing. De toegangsrechten in de Access Control List worden bepaald door de coördinator van iedere huisartsenkring voor wat betreft de gebruikers in zijn huisartsenkring (receptionisten en wachtartsen). Elke wijziging in deze toegangscontrolelijst wordt gelogd. Indien de receptionist overeenkomstig de Access Control List toegangsrechten kan laten gelden, wordt hem toegang verleend. Indien de receptionist niet wordt toegelaten door de Access Control List, wordt hij doorverwezen naar een pagina met een foutbericht.

4. Indien correct geïdentificeerd en geauthenticeerd, kan de gemachtigde receptionist vervolgens volgende gegevens registreren met betrekking tot de patiënt:
   - de identificatiegegevens van de patiënt (manueel, of via uitlezen van de SIS-kaart of eID):
     - identificatienummer van de sociale zekerheid (zijnde het identificatienummer van het Rijksregister dan wel het identificatienummer toegekend door de Kruispuntbank van de sociale zekerheid)
     - naam, voornaam
     - geboortedatum
     - geslacht
     - straat, huisnummer, postcode en woonplaats
     - communicatiegegevens (telefoon, GSM, …)

[1] Als back-up systeem wordt voorzien dat er eveneens met het burgertoken kan worden ingelogd.

- de reden van aanmelding in vrije tekst
- het tijdstip van de oproep
- het type contact:
    - huisbezoek
    - telefonisch
    - consult
- de graad van dringendheid (wachtkamer):
    - niet dringend
    - dringend
    - levensbedreigend
- eigen huisarts van de patiënt (pick-list): achter de picklist (naam, voornaam) zitten de volgende gegevens van de arts:
    - adres: straat, huisnummer, postcode, woonplaats
    - RIZIV nummer
    - houder van een medibridge account (J/N)
    - houder van een eHealthbox account (J/N)

5. Deze gegevens vormen dus de 'wachtkamerlijst' en zijn enkel zichtbaar voor de receptie en de wachtarts. Bij het opmaken van het wachtverslag door de wachtarts worden deze gegevens hierin automatisch geïntegreerd en –indien nodig– verbeterd door de wachtarts. De gegevens in de wachtkamerlijst worden vervolgens definitief verwijderd.

6. De wachtarts die een wachtverslag wenst op te stellen, logt eveneens in door middel van zijn eID[2]. Aan de hand van de gegevens van de eID identificeert en authenticeert het gebruikers- en toegangsbeheer van het eHealth-platform de betrokken persoon en verifieert aan de hand van de gegevens van de federale databank van de beoefenaars van de gezondheidszorgberoepen of de betrokkene effectief geneesheer is. Indien dit het geval is, geeft het gebruikers- en toegangsbeheer van het eHealth-platform vervolgens de identificatiegegevens door aan de Access Control List van de webtoepassing. De Access Control List verifieert of de wachtarts al dan niet toegangsrechten kan laten gelden. Indien dit het geval is, wordt toegang verleend aan de wachtarts tot de toepassing.

7. Indien succesvol aangemeld, opent de wachtarts een nieuw wachtverslag. Indien de functie van receptionist voorzien is en deze de gegevens van de betrokken patiënt in de wachtkamerslijst heeft ingevuld, worden deze gegevens uit de wachtkamerlijst automatisch vooringevuld in het wachtverslag. Indien er geen receptionist is, dan dient de wachtarts alle onderstaande gegevens zelf in te vullen.

8. Indien correct geïdentificeerd en geauthenticeerd, kan de gemachtigde wachtarts volgende gegevens registreren in het wachtverslag:
- de naam/voornaam/woonplaats van de eigen huisarts (ontvanger van het verslag) wordt geselecteerd uit een picklist, waarachter volgende gegevens zitten per arts
    - adres: straat, nr, postcode, woonplaats
    - riziv nummer
    - houder van een medibridge account (ja/neen)
    - houder van een eHealthbox account (ja/neen)
    - patiëntgegevens

[2] Als back-up systeem wordt voorzien dat er eveneens met het burgertoken kan worden ingelogd.

- identificatienummer van de sociale zekerheid (zijnde het identificatienummer van het Rijksregister dan wel het identificatienummer toegekend door de Kruispuntbank van de sociale zekerheid)
- naam, voornaam
- geboortedatum
- geslacht
- straat, nr, postcode, woonplaats
- communicatiegegevens (telefoon, GSM, …)

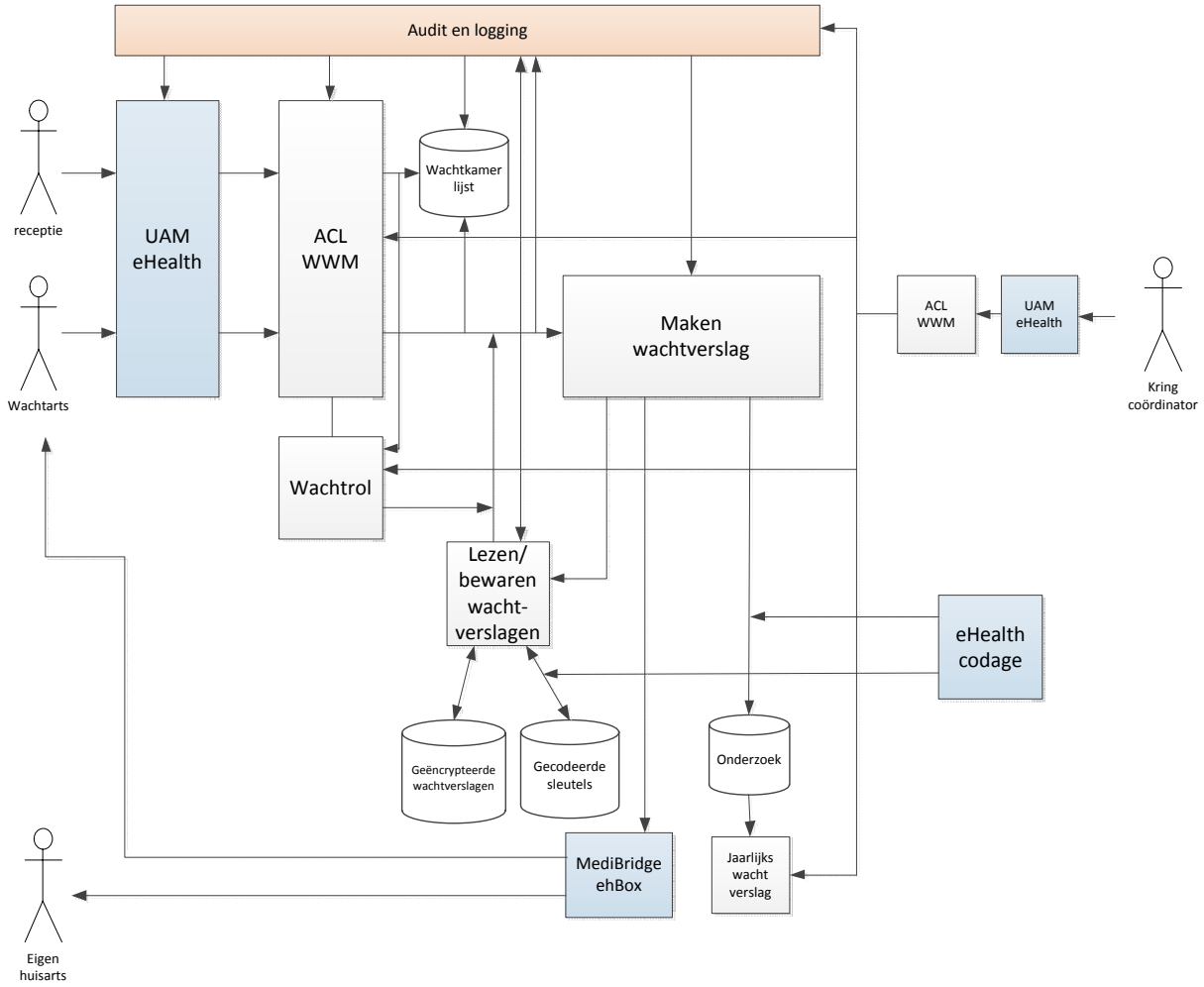
- contactgegevens
  - type contact (huisbezoek/raadpleging/telefonisch contact)
  - tijdstip oproep
  - tijdstip contact met de arts
  - graad van dringendheid (kan wachten tot na de wacht/normaal wachtgebruik/dringend/levensbedreigend)
- medische gegevens
  - subjectieve klachten (=aanmeldingsklachten)
    - IBUI classificatie[3]
    - vrije tekst
  - objectieve vaststellingen
    - vrije tekst
  - evaluatie door arts (=diagnose)
    - IBUI classificatie
    - vrije tekst
  - planning door arts
    - medicatie
      - CNK-code[4]
      - aantal verpakkingen
      - instructies
    - handelingen
      - ICPC2-klasse
      - type: verwijzing, vaccinatie, hechting, ...
      - vrije tekst
    - afwezigheidsattest
      - startdag
      - einddag
      - verlenging (ja/neen)
      - oorzaak (ongeval/ziekte)
      - type (werk/school/sport)
    - vrije tekst
- weigering van de patiënt om toegang te geven tot het wachtverslag tijdens de wachtdienst.[5]

[3] Belgische Unieke Identificator, nummer van een medisch thesaurusterm, dat gelinkt is met een ICP2-code en ICD10-code.
[4] Belgische coderingssysteem voor medicatie.
[5] De toepassing voorziet in de mogelijkheid dat een wachtarts het door een andere wachtarts opgestelde wachtverslag binnen de maand na de creatie van het wachtverslag kan lezen (cfr. infra). De patiënt kan zich hier evenwel uitdrukkelijk tegen verzetten.

9. Aan het wachtverslag wordt de identificatie van de maker van het wachtverslag (de wachtarts), de identificatie van de betrokken wachtkring en een uniek nummer toegevoegd.

10. Vervolgens worden volgende onderdelen van de webtoepassing geactiveerd:
- doorsturen wachtverslag naar eigen huisarts;
- doorsturen eigen kopij wachtverslag naar wachtarts;
- coderen, aggregeren en doorsturen van de gegevens naar de gecodeerde onderzoeksdatabank voor het opstellen van het jaarlijks wachtverslag;
- vercijferen en opslaan van het wachtverslag voor verder gebruik (cfr. infra).

Schematisch kan dit als volgt worden voorgesteld:



11. Nadat de wachtarts het verslag heeft bevestigd, wordt het verstuurd naar de eigen huisarts van de patiënt via de diensten van een softwareontwikkelaar[6].

12. Nadat het verslag bevestigd is, giet de wachtverslagmodule de gegevens in een specifiek formaat. De aanvrager stelt dat elk softwarepakket voor het beheer van het elektronische medisch dossier door huisartsen dit formaat kan integreren.

[6] Medibridge.

13. Het verslag wordt vervolgens asymmetrisch geëncrypteerd door middel van de encryptiedienst van voormelde softwareontwikkelaar en wordt verstuurd aan de hand van het RIZIV-nummer naar de eigen huisarts van de patiënt. Het bericht wordt gedecrypteerd bij de eigen huisarts door zijn eigen programma. Daarna wordt het automatisch geïntegreerd in het elektronisch medisch dossier van de betrokken patiënt.

14. Indien de eigen huisarts geen gebruik zou maken van de diensten van voormelde softwareontwikkelaar wordt het verslag uitgeprint bij de wachtarts. Deze stuurt het verslag dan per post naar de eigen huisarts of geeft deze met de patiënt mee.

15. Aangezien de wachtarts een kopij moet bewaren van zijn eigen wachtverslag, is het noodzakelijk dat hij deze eveneens toegestuurd krijgt. De wijze van verzending is gelijk aan die voor de huisarts.

16. In een latere fase zal de webtoepassing de wachtverslagen meedelen aan de huisarts en de betrokken wachtarts door middel van de beveiligde elektronische brievenbus van het eHealth-platform, de eHealth-box.

17. Een selectie van de gegevens van het wachtverslag wordt meegedeeld aan een centrale onderzoeksgegevensbank. Deze is enkel toegankelijk voor coördinatoren van de huisartsenkringen voor het opmaken van het jaarlijks wachtverslag, waarbij de betrokken coördinatoren enkel de wachtverslagen van hun eigen huisartsenkring kunnen consulteren. Overeenkomstig artikel 7 van het koninklijk besluit van 8 juli 2002 *tot vaststelling van de opdrachten verleend aan huisartsenkringen* is elke huisartsenkring immers verplicht een registratie te organiseren omtrent volgende gegevens in relatie tot de organisatie van de wachtdienst : epidemiologie, veiligheidsproblemen, patiëntenklachten, klachten omtrent dienstverlening. Deze rapportering, die enkel anonieme en geaggregeerde gegevens bevat, wordt vervolgens door iedere kringcoördinator verstuurd naar de federale overheidsdienst volksgezondheid, veiligheid van de voedselketen en leefmilieu en bevat enkel anonieme geaggregeerde gegevens.

18. Alvorens de selectie van gegevens wordt overgemaakt aan de onderzoeksgegevensbank wordt het identificatienummer van de sociale zekerheid (INSZ) van de betrokkene gecodeerd door middel van de basisdienst 'codering en anonimisering' van het eHealth-platform. Het eHealth-platform bewaart de link tussen het INSZ en het gecodeerde nummer teneinde longitudinaal onderzoek mogelijk te maken doch er wordt niet voorzien in de mogelijkheid tot decodering.

19. De gecodeerde onderzoeksgegevensbank bevat de volgende gegevens per wachtverslag:
    - gecodeerd identificatienummer van de sociale zekerheid (identificatienummer van het Rijksregister dan wel identificatienummer toegekend door de Kruispuntbank van de sociale zekerheid)
    - wachtkringidentificatienummer tot dewelke de verzendende wachtarts behoort
    - patiëntgegevens
        - geslacht
        - postcode
        - leeftijdsklasse ('0','1-4','5-9','10-14','15-19','20-24','25-29','30-34','35-39','40-44','45-49','50-54','55-59','60-64','65-69','70-74','75-79','80-84','85-89','90-94','95+','O')
    - contactgegevens
        - type contact (huisbezoek/raadpleging/telefonisch contact)

- tijd tussen oproep en contact met de arts
- geaggregeerd tijdstip contact met de arts:
    - jaartal
    - weeknummer
    - weekend of midweek
    - uur van contact
- graad van dringendheid (kan wachten tot na de wacht/normaal wachtgebruik/dringend/levensbedreigend

- medische gegevens
    - subjectieve klachten (=aanmeldingsklachten) : IBUI classificatie
    - evaluatie door arts (=diagnose) : IBUI classificatie
- verwijzing
    - RIZIV-nummer instelling

20.1. De gecodeerde persoonsgegevens worden in de onderzoeksgegevensbank slechts bewaard voor de duur van anderhalf jaar, meer bepaald de tijd die nodig is voor het opmaken van het jaarlijks wachtverslag.

20.2. De toepassing voorziet er eveneens in dat de wachtverslagen op vercijferde wijze worden bewaard op een centrale server voor twee doeleinden:

- de wachtarts moet altijd een verslag hebben van de door hem uitgevoerde consult. Hoewel hij, zoals hoger beschreven, een elektronische kopie ontvangt, heeft volgens de aanvrager het verleden aangetoond dat door technische problemen wachtverslagen verloren zijn gegaan. Daarom worden de wachtverslagen op een server bewaard voor een looptijd van één jaar, waarna ze onherroepelijk worden vernietigd. De gebruiker die als wachtarts is opgetreden wordt per mail meermaals verwittigd dat deze verslagen moeten worden afgehaald. Enkel de auteur van het wachtverslag kan voor dit doeleinde het wachtverslag opvragen.

- daarnaast is het voor de continuïteit van de zorg noodzakelijk dat een wachtarts de wachtverslagen kan lezen van een patiënt bij een *herconsultatie,* bijvoorbeeld in volgende gevallen:

- een palliatieve patiënt bij dewelke een wachtarts mogelijke meerdere keren per dag langskomt;
- een patiënt die telefonisch uitleg vraagt over een voorbijgaand consult;
- een patiënt die de wachtarts informeert over het vervolg van zijn/haar toestand van de ziekte;
- een tweede consult tijdens het weekend voor hetzelfde probleem.

Aangezien voor dit doeleinde de wachtverslagen slechts een beperkt nut hebben in tijd, zijn ze slecht oproepbaar tot één maand na het opmaken van het wachtverslag.

20.3. De wachtverslagen worden voor de voormelde doeleinden op vercijferde wijze opgeslagen op een centrale server zodat uitsluitend gemachtigde gebruikers toegang kunnen hebben tot de inhoud van de verslagen (cfr. infra). Gelet op het feit dat de wachtverslagen op vercijferde wijze worden bewaard, kunnen de beheerders van de server geen kennis nemen van de wachtverslagen.

II. BEVOEGDHEID

21. Artikel 11 van de wet van 21 augustus 2008 *houdende oprichting en organisatie van het eHealth-platform* bepaalt dat elke mededeling van persoonsgegevens door of aan het eHealth-platform, behoudens enkele uitzonderingsgevallen, een principiële machtiging van de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid vereist.

22. De mededeling van persoonsgegevens door of aan het eHealth-platform in het kader van de basisdienst 'gebruikers- en toegangsbeheer' werd gemachtigd door het Sectoraal comité bij beraadslaging nr. 09/008 van 20 januari 2009[7].

23. Overeenkomstig artikel 42, §2, 3° van de wet van 13 december 2006 houdende diverse bepalingen betreffende gezondheid is de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid bevoegd voor het verlenen van een principiële machtiging met betrekking tot elke mededeling van persoonsgegevens die de gezondheid betreffen in de zin van de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna genoemd: "de wet van 8 december 1992")**.**

24. De mededeling persoonsgegevens die de gezondheid betreffen, vereist evenwel geen machtiging indien het gebeurt tussen beroepsbeoefenaars in de gezondheidszorg die door het beroepsgeheim gebonden zijn en persoonlijk betrokken zijn bij de uitvoering van diagnostische, preventieve of zorgverlenende handelingen ten opzichte van een patiënt.

25. De mededeling van persoonsgegevens die de gezondheid betreffen tussen de wachtarts en de huisarts van de betrokken patiënt in de vorm van het wachtverslag vereist bijgevolg geen machtiging van het Sectoraal comité. Het onderzoek van het Sectoraal comité beperkt zich bijgevolg tot de verwerking van persoonsgegevens door de webtoepassing WebWachtMailer en de mededeling van –gecodeerde– persoonsgegevens die de gezondheid betreffen door deze webtoepassing aan de onderzoeksgegevensbank in het kader van het opstellen van de jaarlijkse rapportering door de kringcoördinatoren.

26.1. Hoewel de mededeling van het wachtverslag tussen de wachtarts en huisarts buiten haar bevoegdheid valt, wijst het Sectoraal comité er op dat iedere wachtarts alleszins rekening dient te houden met de toepasselijke wetgeving met betrekking tot de geoorloofdheid van de mededeling van het wachtverslag aan de huisarts. Het verwijst hierbij expliciet naar de wet van 2 augustus 2002 *betreffende de rechten van de patiënt*, de code van geneeskundige plichtenleer van de Nationale Orde der Geneesheren en vanzelfsprekend naar wet van 8 december 1992.

26.2. Het eHealth-platform staat tot slot in voor de codering van het identificatienummer van de sociale zekerheid, waarbij het verband tussen dit nummer en het gecodeerd nummer wordt bewaard. Overeenkomstig artikel 5, 8°, van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform mag het *eHealth*-platform

[7] Beraadslaging nr. 09/008 van 20 januari 2009, gewijzigd op 16 maart 2010 en op 15 juni 2010, van het sectoraal comité van de sociale zekerheid en van de gezondheid met betrekking tot de toepassing van het geïntegreerd gebruikers- en toegangsbeheer door het eHealth-platform bij de uitwisseling van persoonsgegevens.

evenwel het verband tussen het reële identificatienummer van een betrokkene en het aan hem toegekend gecodeerd identificatienummer slechts bijhouden indien de bestemmeling van de gecodeerde persoonsgegevens daarom op een gemotiveerde wijze verzoekt, mits machtiging van de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid.

III. BEHANDELING

A. FINALITEIT

27. Artikel 4, §1, 1°, van de wet van 8 december 1992 stelt dat iedere verwerking van persoonsgegevens eerlijk en rechtmatig dient te zijn. Bovendien staat artikel 4, §1, 2°, van de wet van 8 december 1992 de verwerking slechts toe voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

28. Hermes vzw die optreedt als verantwoordelijke voor de verwerking heeft overeenkomstig haar statuten tot doel:
- studies in verband met de problematiek van de uitoefening van het beroep als huisarts opzetten of eraan meewerken;
- meewerken aan de universitaire en postuniversitaire wetenschappelijke vorming van de huisarts;
- de wetenschappelijke onderzoekingen door huisartsen bevorderen;
- de praktijkvoering door huisartsen ondersteunen.

29. Hierbij mag de vereniging alle mogelijke activiteiten inrichten of eraan deelnemen voor zover zij gericht zijn op het bereiken van de doelstellingen van de vzw..

30. De webtoepassing die ter beschikking wordt gesteld door Hermes vzw heeft vooreerst tot doel in het kader van de door de huisartsenkringen wettelijk verplicht te organiseren wachtdiensten[8] een wachtverslag on-line op te stellen en dit wachtverslag over te maken (elektronisch dan wel op papier) aan enerzijds de huisarts van de betrokken patiënt en anderzijds de wachtarts zelf.

31. Daarnaast heeft de webtoepassing tot doel om een selectie van de gegevens afkomstig van het via de webtoepassing gecreëerde wachtverslag op te slaan in een gegevensdatabank die uitsluitend kan worden geconsulteerd door de coördinatoren van de huisartsenkringen in het kader van de wettelijk verplichte jaarlijkse rapportering aan de federale overheidsdienst volksgezondheid.

32. Het Comité is bijgevolg van oordeel dat het nagestreefde doeleinde van de verwerking door de aanvrager welbepaald, uitdrukkelijk omschreven en gerechtvaardigd is.

B. PROPORTIONALITEIT

[8] Afdeling II, koninklijk besluit van 8 juli 2002 *tot vaststelling van de opdrachten verleend aan huisartsenkringen.*

33. Artikel 4, §1, van de wet van 8 december 1992 stelt eveneens dat de persoonsgegevens die worden verwerkt toereikend, terzake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt. Ze dienen bovendien nauwkeurig te zijn en, zo nodig, te worden bijgewerkt. Alle redelijke maatregelen dienen te worden getroffen om de gegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren.

34. Wat betreft de mededeling van persoonsgegevens die de gezondheid betreffen aan de onderzoeksgegevensbank, motiveert de aanvrager dat de beoogde persoonsgegevens noodzakelijk zijn voor het opstellen van het jaarlijks verslag door de kringcoördinators. Deze laatsten moeten onder andere volgende elementen in het verslag kunnen opnemen:
- regio van waar de patiënt komt (komen ze uit de eigen wachtkring of de naburige wachtkring);
- leeftijdspiramide gespreid volgens geslacht;
- reële noodzaak van wachtdienstgebruik (per leeftijdsgroep);
- aantal huisbezoeken/raadplegingen/telefonische consulten ingedeeld per regio van de patiënt;
- incidentie van de pathologieën waarvoor de patiënt komt per leeftijdsgroep;
- incidentie van de pathologieën die gediagnosticeerd zijn door de arts per leeftijdsgroep;
- wachttijd van de patiënt (tijd tussen oproep en contact) ingedeeld per urgentiegraad;
- gebruiksfrequentie wachtdienst ingedeeld per:
    - midweek en weekend;
    - week van het jaar;
    - uur van de dag.

35.1. Wat betreft de bewaartermijn van de gegevens, worden de gegevens in de onderzoeksgegevensbank slechts bewaard gedurende maximaal anderhalf jaar, namelijk de tijd die nodig is voor het opmaken van de jaarlijkse rapportering.

35.2. De aanvrager argumenteert dat het gecodeerd identificatienummer van de sociale zekerheid eveneens in de onderzoeksdatabase dient te worden opgenomen teneinde de patiënten op unieke wijze te kunnen identificeren en aan de hand hiervan de demografische en pathologische gegevens van patiënten die repetitief terugkomen tijdens de wachtdienst te kunnen analyseren. Het Sectoraal comité acht het aanvaardbaar dat de betrokkenen op unieke –gecodeerde- wijze worden geïdentificeerd voor dit doeleinde.

36. Concluderend kan gesteld worden dat het Sectoraal comité de persoonsgegevens die worden verwerkt toereikend, terzake dienend en niet overmatig acht.

37. Zoals reeds vermeld, behoeft de mededeling van persoonsgegevens die de gezondheid betreffen tussen de wachtarts en de huisarts geen machtiging. Desalniettemin dient te worden onderzocht in hoeverre de verwerking van de persoonsgegevens door de webtoepassing zelf voldoet aan het principe van proportionaliteit, en dan meer bepaald de tijdelijke opslag van de vercijferde wachtverslagen.

38. De gegevens geregistreerd door de receptioniste, indien aanwezig, in de wachtkamerlijst worden slechts bewaard op de server van de webtoepassing totdat deze zijn geïntegreerd

in het wachtverslag. Vervolgens worden de gegevens van de wachtkamerlijst onherroepelijk verwijderd.

39.1. Het wachtverslag zelf wordt opgeslagen op de server van de webtoepassing. Het Sectoraal comité acht het aanvaardbaar dat de wachtverslagen worden bewaard respectievelijk één jaar voor consultatie door de wachtarts zelf, en één maand voor iedere andere wachtarts die kan aantonen dat hij een consult aan de patiënt heeft verleend.

39.2. De wachtverslagen worden op vercijferde wijze bewaard. De aanvrager omschrijft de werkwijze als volgt:
- eerst wordt een *random key* aangemaakt;
- deze *key* vercijfert het wachtverslag, het vercijferde wachtverslag wordt bewaard op de server. De vercijfering wordt uitgevoerd aan de hand van het AES256 algoritme;
- de *key* wordt verzonden naar de dienst "codage" van het eHealth-platform. De geeft een gecodeerde *key* terug. De gecodeerde *key* wordt bewaard op de server. Met deze gecodeerde *key* is het niet mogelijk om het wachtverslag te ontcijferen.
- de originele key wordt vernietigd

39.3. Om een wachtverslag tijdens een wachtdienst te kunnen consulteren, moet aan de volgende voorwaarden worden voldaan:
- de arts die een wachtverslag opent, moet overeenkomstig het gebruikers- en toegangsbeheer van wacht zijn.
- de arts die een wachtverslag opent moet een therapeutische relatie hebben met de betrokken persoon. Dit wordt *post-hoc* gecontroleerd door na te kijken of hij een wachtverslag gemaakt heeft.
- het wachtverslag mag niet ouder zijn dan 1 maand (wachtverslagen ouder dan één maand verschijnen ook niet in de zoekresultaten).
- de patiënt mag niet geweigerd hebben dat het wachtverslag nadien mag heropend worden (zie randnummer 8).

39.4. Technisch gezien verloopt de ontcijfering als volgt:
- het vercijferd wachtverslag wordt met zijn gecodeerde sleutel uit de database gehaald ;
- de gecodeerde sleutel wordt gedecodeerd door het eHealth platform ;
- de gedecodeerde sleutel (= originele sleutel) wordt gebruikt om het wachtverslag te ontcijferen (AES256) en wordt daarna vernietigd ;
- het gedecrypteerde wachtverslag is hiermee beschikbaar.

39.5. De post-hoc controle heeft als doel te verifiëren of een gebruiker een therapeutische relatie had op het ogenblik dat hij een dossier van een patiënt opende. Een therapeutische relatie wordt in het kader van deze webtoepassing bevestigd door na het consult een wachtverslag te versturen in hoofde van de betrokken patiënt.

De post-hoc controle kijkt na of voor elk geopend verslag van een patiënt door een gebruiker, nadien ook door dezelfde gebruiker een wachtverslag verstuurd is voor deze patiënt. Bij de gebruikers die dit niet gedaan hebben, wordt de kringcoördinator hiervan verwittigd..

Technisch gezien worden alle wachtverslagen die niet door de auteur zijn geopend, gelogd in de "post-hoc controle database".

Een batch proces overloopt voor elk element in deze “post-hoc controle database” of er in de 24 uur die erop volgt een wachtverslag is gemaakt voor deze patiënt door de wachtarts die het verslag heeft geopend. Indien dit niet het geval is, wordt de kringcoördinator hiervan per mail verwittigd.

Dit batch proces wordt uitgevoerd elke weekdag om 12 uur.

De kringcoördinator heeft als taak de rapportering van de ongeldig geopende wachtverslagen te onderzoeken en deze door te geven aan het bestuur van de wachtkring zodat deze een sanctie kan opleggen.

40. Gelet op het voorgaande acht het Sectoraal comité wat betreft de verwerking van persoonsgegevens in het kader van de webtoepassing de persoonsgegevens die worden verwerkt toereikend, terzake dienend en niet overmatig.

41. De resultaten van de jaarlijkse wachtverslagen mogen niet worden bekendgemaakt in een vorm die de identificatie van de betrokken persoon mogelijk maakt. De kringcoördinatoren zijn bijgevolg gehouden in de jaarlijkse rapportering alle mogelijke gegevens die tot de identificatie van de betrokkenen zouden kunnen leiden, te verwijderen.

42. Overeenkomstig artikel 7 van de wet van 8 december 1992 is de verwerking van persoonsgegevens die de gezondheid betreffen, in beginsel verboden. Dit verbod is echter niet van toepassing, o.a.:
    - wanneer de verwerking om redenen van zwaarwegend algemeen belang verplicht wordt door of krachtens een wet, een decreet of een ordonnantie, hetgeen het geval is voor het opstellen van het jaarlijks wachtverslag;
    - wanneer de verwerking noodzakelijk is voor doeleinden van preventieve geneeskunde of medische diagnose, het verstrekken van zorg of behandelingen aan de betrokkene of een verwant, of het beheer van de gezondheidsdiensten handelend in het belang van de betrokkene en de gegevens worden verwerkt onder het toezicht van een beroepsbeoefenaar in de gezondheidszorg, hetgeen het geval is voor het opmaken en overmaken van het wachtverslag aan de huisarts.

43. Wat betreft de vereiste dat de verwerking wordt uitgevoerd onder een verantwoordelijkheid van een beroepsbeoefenaar in de gezondheidszorg, neemt het Sectoraal comité akte van het feit dat de verwerking van de persoonsgegevens die de gezondheid betreffen in het kader van de webtoepassing WebWachtMailer plaatsvindt onder de verantwoordelijkheid van een geneesheer. Bijgevolg is voldaan aan voormelde vereiste.

C. TRANSPARANTIE

44. Wat betreft de verwerking van de persoonsgegevens in het kader van de onderzoeksgegevensbank, voorziet artikel 9 van de wet van 8 december 1992 in een verplichting tot informatie van de betrokken personen van wie persoonsgegevens worden verwerkt.

45. De verantwoordelijke voor de verwerking wordt van de kennisgeving vrijgesteld wanneer de registratie of de verstrekking van de persoonsgegevens verricht wordt met het oog op de toepassing van een bepaling voorgeschreven door of krachtens een wet, een decreet of een ordonnantie.

46. Gelet op het feit dat de gegevensverwerking plaatsvindt in het kader van de wettelijke verplichte redactie van jaarlijkse wachtverslag, acht het Sectoraal comité de verantwoordelijke van de verwerking vrijgesteld om de betrokkene te informeren.

D. VEILIGHEIDSMAATREGELEN

47. Overeenkomstig artikel 16 van de wet van 8 december 1992 moet de verantwoordelijke voor de verwerking van de webtoepassing, zijnde Hermes vzw, 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.

48. Indien de verwerking wordt toevertrouwd aan een verwerker dient de verantwoordelijke een verwerker te kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking. De verantwoordelijke dient toe te zien op de naleving van die maatregelen, met name door ze vast te leggen in contractuele bepalingen. Hij dient de aansprakelijkheid van de verwerker ten aanzien van de verantwoordelijke voor de verwerking vast te stellen in de overeenkomst. De verantwoordelijke dient met de verwerker verder overeen te komen - in een geschrift of op een elektronische drager - dat de verwerker slechts handelt in opdracht van de verantwoordelijke voor de verwerking en dat de verwerker is gebonden door dezelfde verplichtingen als deze die waartoe de verantwoordelijke in toepassing van artikel 16, §3 van de wet van 8 december 1992 is gehouden.

49. Voor de tijdelijke opslag van de gegevens van de wachtkamerlijst, van de wachtverslagen evenals van de onderzoeksgegevensbank maakt Hermes vzw gebruik van een server die wordt beheerd door het Universitair Ziekenhuis Leuven (UZLeuven). Hermes vzw is bijgevolg als verantwoordelijke voor de verwerking gehouden een schriftelijke overeenkomst af te sluiten met het UZLeuven waarin voormelde elementen zijn opgenomen. Een kopie van deze overeenkomst dient ter beschikking te worden gehouden van het Sectoraal comité.

50. Het Sectoraal comité wijst er op dat eenieder die handelt onder het gezag van de verantwoordelijke voor de verwerking of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verantwoordelijke voor de verwerking mag verwerken, behoudens op grond van een verplichting door of krachtens een wet, een decreet of een ordonnantie.

51. Wat betreft de implementatie van de gepaste technische en organisatorische maatregelen verwijst het Sectoraal comité naar de referentiemaatregelen die door de Commissie tot bescherming van de persoonlijke levenssfeer zijn opgesteld voor de beveiliging van elke

verwerking van persoonsgegevens[9]. Het betreft een lijst met tien actiedomeinen in verband met de informatiebeveiliging waarvoor elke instelling – rechtspersoon, onderneming of administratie – die persoonsgegevens bewaart, verwerkt of mededeelt, maatregelen moet nemen. Overeenkomstig deze referentiemaatregelen dient de instelling te beschikken over een geschreven veiligheidsbeleid waarin de strategieën en de weerhouden maatregelen voor gegevensbeveiliging nauwkeurig worden omschreven. Er moet een veiligheidsconsulent worden aangesteld die verantwoordelijk is voor de uitvoering van het veiligheidsbeleid. De instelling moet duidelijk de verantwoordelijkheden en het beheersproces inzake beveiliging van persoonsgegevens omschrijven en deze op gepaste wijze integreren in de algemene organisatiestructuur en werking. De instelling moet de nodige maatregelen nemen om de fysieke bescherming van de persoonsgegevens te garanderen. De instelling moet zich ervan vergewissen dat de netwerken waarmee de apparatuur verbonden is en die betrokken is bij een verwerking van persoonsgegevens, de vertrouwelijkheid en de integriteit van de gegevens garanderen. De instelling moet zich ervan vergewissen dat de persoonsgegevens overeenkomstig hun classificatie slechts toegankelijk zijn voor de personen en toepassingsprogramma's die hiertoe uitdrukkelijk gemachtigd zijn. De instelling moet loggings- en opsporingsmechanismen installeren. De instelling moet zich ervan vergewissen dat de technische of organisatorische veiligheidsmaatregelen gevalideerd zijn en regelmatig nagekeken worden. De instelling moet beschikken over een beheersplan voor veiligheidsincidenten. Tot slot, moet de instelling beschikken over een volledige, gecentraliseerde documentatie en deze met betrekking tot de veiligheid regelmatig bijwerken.

52. Wat betreft de verwerking door het UZLeuven, neemt het Sectoraal comité akte van het feit dat het UZLeuven eveneens beschikt over een veiligheidsconsulent. Wat betreft de beveiliging van netwerken waarmee de apparatuur verbonden is en die betrokken is bij een verwerking van persoonsgegevens, wordt voorzien dat via de firewall van het UZLeuven enkel de http en https poorten toegankelijk zijn vanaf het internet. Via de remote access faciliteiten van het UZLeuven wordt er voor gezorgd dat enkel geautoriseerde personen via een virtueel privé-netwerk (VPN) toegang kunnen krijgen tot alle netwerkpoorten van de apparatuur. Voor de authenticatie moeten deze personen gebruik maken van hun persoonlijke token. Hierbij wordt door het UZLeuven gelogd wanneer en door wie een dergelijke verbinding wordt opgezet. De hardware van de servers wordt opgesteld in een datacenter waar enkel bevoegde personen toegang hebben en dat is voorzien van automatische brandblusinstallaties en noodstroomvoorzieningen. Tot slot neemt het Comité akte van het feit dat de betrokken personeelsleden van UZLeuven geen toegang hebben tot de persoonsgegevens in de webtoepassing zelf.

53. Op het niveau van de webtoepassing zelf, wordt een specifiek loggingsysteem voorzien dat logt welke gebruiker welke handeling uitvoert op welk tijdstip.

54. Wat betreft de geclassificeerde toegang tot de gegevens wordt gebruik gemaakt van de basisdienst 'gebruikers- en toegangsbeheer' van het eHealth-platform voor de identificatie en authenticatie van de gebruikers aan de hand van hun eID en voor de verificatie van de hoedanigheid als geneesheer in de federale databank van de beoefenaars van een gezondheidszorgberoep. Na identificatie en authenticatie volgt een verificatie aan de hand van de *Access Control List* waarin de toegangsrechten van de

[9] http://www.privacycommission.be/en/static/pdf/referenciemaatregelen-vs-01.pdf

kringcoördinator, de wachtartsen en de receptionisten zijn vastgelegd, alvorens de betrokkenen de gegevens in kwestie kunnen raadplegen.

55. De kringcoördinator beheert de toegang van de leden van zijn huisartsenkring (receptie en wachtarts) aan de hand van de toegangscontrolelijst (*Access Control List*). Hij beheert de toegangsrechten: hij voegt nieuwe gebruikers toe of verwijdert hen wanneer noodzakelijk. Hij verwijdert eveneens de gebruikers op vraag van de huisartsenkring, Hermes vzw of op eigen initiatief in geval van onrechtmatig gebruik door de betrokken gebruiker. Elke wijziging in de toegangscontrolelijst wordt eveneens gelogd.

56. Uitsluitend de receptionist en de wachtarts hebben toegang tot de wachtkamerlijst van de hen betreffende patiënten. De wachtarts en de receptionist hebben daarnaast ook toegang tot het logboek van hun respectievelijke acties. Een wachtarts heeft conform de hoger beschreven regels toegang tot de wachtverslagen. De kringcoördinator tot slot heeft toegang tot het logboek van de gebruikers van zijn kring en heeft toegang tot de onderzoeksgegevensbank met betrekking tot de wachtverslagen opgesteld door wachtartsen uit zijn kring.

57. Het Sectoraal comité stelt vast dat Hermes een overeenkomst afsluit met betrekking tot het gebruik van de webtoepassing zowel met iedere wachtkring (verplicht opgericht als vereniging zonder winstgevend doel), als met iedere kringcoördinator en gebruiker. Het Sectoraal comité mocht een kopie ontvangen van de modellen van voormelde overeenkomsten.

58. Het Sectoraal comité wijst er op dat overeenkomstig artikel 458 van het Strafwetboek alle personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, en deze bekendmaken buiten het geval dat zij geroepen worden om in rechte of voor een parlementaire onderzoekscommissie getuigenis af te leggen en buiten het geval dat de wet hen verplicht die geheimen bekend te maken, gestraft worden met gevangenisstraf en met geldboetes. Bovendien is het overeenkomstig artikel 6 van het koninklijk besluit van 13 februari 2001 *ter uitvoering van de wet van 8 december 1992* verboden om handelingen te stellen die ertoe strekken de meegedeelde gecodeerde persoonsgegevens om te zetten in niet-gecodeerde persoonsgegevens. Er wordt op gewezen dat het niet naleven van dit verbod, krachtens artikel 39, 1°, van de wet van 8 december 1992, een geldboete tot gevolg kan hebben. Het Sectoraal comité wijst er op dat overeenkomstig artikel 5 van het wetboek van strafvordering eveneens rechtspersonen strafrechtelijk aansprakelijk kunnen worden gesteld voor misdrijven die hetzij een intrinsiek verband hebben met de verwezenlijking van zijn doel of de waarneming van zijn belangen, of die, naar blijkt uit de concrete omstandigheden, voor zijn rekening zijn gepleegd.

59. Tot slot zijn zowel Hermes vzw als de UZLeuven ertoe gehouden alle personen die onder hun gezag handelen goed te informeren over de bepalingen van de wet van 8 december 1992 en van de uitvoeringsbesluiten ervan alsook over elk relevant voorschrift met betrekking tot de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

60. Indien correct en volledig toegepast, acht het Comité voormelde veiligheidsmaatregelen toereikend om de vertrouwelijkheid en de veiligheid van de gegevensverwerking te

waarborgen in het licht van de bepalingen van artikel 16 van de wet van 8 december 1992.

Om deze redenen,

verleent de afdeling gezondheid van het sectoraal comité van de sociale zekerheid en van de gezondheid,

onder de in deze beraadslaging opgenomen voorwaarden, de machtiging tot de verwerking van de hogervermelde persoonsgegevens in het kader van de webtoepassing WebWachtMailer.

Het Sectoraal comité machtigt het eHealth-platform het verband tussen het reële identificatienummer van de betrokkenen en de aan hen toegekende gecodeerde identificatienummers bij te houden.

Yves ROGER
Voorzitter