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

SCSZ/10/101

ADVIES NR 10/21 VAN 7 SEPTEMBER 2010 BETREFFENDE DE VRAAG VAN DE MINISTER VAN SOCIALE ZAKEN MET BETREKKING TOT HET PROTOCOL, OPGEMAAKT OP 17 MAART 2010 DOOR DE OVEREENKOMSTENCOMMISSIE VERPLEEGKUNDIGEN-VERZEKERINGSINSTELLINGEN, HOUDENDE DE VOORWAARDEN EN MODALITEITEN VOLGENS DEWELKE BEWIJSKRACHT KAN WORDEN GEGEVEN TOT HET BEWIJS VAN HET TEGENDEEL AAN GEGEVENS DIE WORDEN OPGESLAGEN OF BEWAARD DOOR MIDDEL VAN EEN ELEKTRONISCHE TECHNIEK OF WORDEN MEEGEDEELD OP EEN ANDERE WIJZE DAN OP EEN PAPIEREN DRAGER, EVENALS DE VOORWAARDEN EN MODALITEITEN VOLGENS WELKE DEZE GEGEVENS WORDEN WEERGEGEVEN OP PAPIEREN DRAGER OF OP ELKE ANDERE LEESBARE DRAGER

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*;

Gelet op het koninklijk besluit van 27 april 1999 *betreffende de bewijskracht van de door de zorgverleners, de verzekeringsinstellingen, het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering en andere natuurlijke of rechtspersonen met toepassing van gecoördineerde wet van 14 juli 1994 betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen en haar uitvoeringsbesluiten opgeslagen, verwerkte, weergegeven of meegedeelde gegevens*;

Gelet op de aanvraag van het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering;

Gelet op het auditoraatsrapport van de Kruispuntbank van de Sociale Zekerheid van 23 augustus 2010;

Gelet op het verslag van de heer Yves Roger.

A. SITUERING VAN DE AANVRAAG

1. Artikel 2 van het koninklijk besluit van 27 april 1999 *betreffende de bewijskracht van de door de zorgverleners, de verzekeringsinstellingen, het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering en andere natuurlijke of rechtspersonen met toepassing van gecoördineerde wet van 14 juli 1994 betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen en haar uitvoeringsbesluiten opgeslagen, verwerkte, weergegeven of meegedeelde gegevens* bepaalt dat, voor toepassing van de verplichte verzekering voor geneeskundige verzorging en uitkeringen, de gegevens waarover de zorgverleners, de verzekeringsinstellingen, het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering of alle andere natuurlijke personen of rechtspersonen beschikken en die zijn opgeslagen of bewaard door middel van een elektronische, fotografische, optische of elke andere techniek, of die worden meegedeeld op een andere dan op een papieren drager, evenals hun weergave op papier of op elke andere leesbare drager, bewijskracht hebben tot bewijs van het tegendeel, indien de procedure volgens welke de voormelde opslag, bewaring of mededeling gebeurt, overeenstemt met de procedure die wordt beschreven in het protocol dat tot stand komt met inachtneming van het bepaalde in artikel 3 en wordt goedgekeurd door de Minister krachtens artikel 9.

2. Krachtens artikel 9 van bovenvermeld koninklijk besluit zal de Minister onder meer nagaan of de beschreven procedure aan volgende voorwaarden voldoet:

1) de voorgestelde procedure waarborgt een getrouwe, duurzame en volledige weergave van de informatie;
2) de procedure voorziet een systematische en volledige registratie van de gegevens;
3) de procedure voorziet dat de gegevens op een zorgvuldige manier worden bewaard, systematisch worden gerangschikt en worden beschermd tegen vervalsing en voorziet veiligheidsmaatregelen om het vertrouwelijk karakter van de gegevens te beschermen;
4) de procedure voorziet dat volgende gegevens met betrekking tot verwerking van de gegevens worden bewaard:
    a) de identiteit van de verantwoordelijke voor de verwerking evenals van diegene die ze heeft uitgevoerd;
    b) de aard en het onderwerp van de informatie waarop de verwerking betrekking heeft;
    c) de datum en de plaats van de verrichting;
    d) de eventuele storingen die zijn vastgesteld tijdens de verwerking.

3. Krachtens artikel 3 van datzelfde koninklijk besluit wordt het bovenvermelde protocol opgemaakt door de overeenkomsten- of akkoordencommissie van het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering, in verband met de categorie van zorgverleners waarvoor zij de bevoegdheid heeft een akkoord of overeenkomst te sluiten. Dit protocol bevat een nauwkeurige omschrijving van de voorwaarden en modaliteiten volgens welke gegevens, nodig voor de toepassing van de verplichte verzekering voor geneeskundige verzorging en waarover de voornoemde zorgverleners en de verzekeringsinstellingen beschikken, kunnen worden opgeslagen of bewaard door middel van een elektronische, fotografische, optische of elke andere techniek of meegedeeld op een andere wijze dan op

een papieren drager, evenals de voorwaarden en modaliteiten volgens dewelke deze gegevens worden weergegeven op papier of op elke andere leesbare drager.

Het protocol wordt door de betrokken akkoorden- en overeenkomstencommissie ter goedkeuring voorgelegd aan de Minister van Sociale Zaken. Alvorens een beslissing te nemen, legt de Minister het protocol voor aan het sectoraal comité van de sociale zekerheid en van de gezondheid, dat hem zijn eventuele opmerkingen binnen een termijn van twee maanden bezorgt.

4. Met een schrijven van 6 april 2010 heeft het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering de Minister van Sociale Zaken het protocol inzake de bewijskracht van elektronische gegevens in de thuisverpleging MyCareNet voorgelegd, in uitvoering van het koninklijk besluit van 27 april 1999.

Overeenkomstig artikel 9 van voorvermeld koninklijk besluit werd het protocol inmiddels voor advies voorgelegd aan het sectoraal comité van de sociale zekerheid en van de gezondheid.

Het sectoraal comité van de sociale zekerheid en van de gezondheid heeft de Minister geïnformeerd over het feit dat er met het oog op het formuleren van een gemotiveerd advies bijkomende informatie omtrent het voorgelegde protocol moest worden bekomen vanwege het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering en het Nationaal Intermutualistisch College. Deze inlichtingen[1] werden door de Minister aan het sectoraal comité overgemaakt op 8 juli 2010.

B. BEHANDELING VAN DE AANVRAAG

5. Het protocol dient te worden getoetst aan de technische voorwaarden vermeld in artikel 9 van het hogervermeld koninklijk besluit van 27 april 1999.

Het voorgelegde protocol bepaalt de voorwaarden en modaliteiten waaraan de procedure van de gegevensoverdracht tussen verpleegkundigen en verzekeringsinstellingen dient te voldoen opdat aan de hierna opgesomde gegevens die worden opgeslagen of bewaard door middel van een elektronische, fotografische, optische of elke andere techniek of meegedeeld op een andere wijze dan op een papieren drager bewijskracht tot bewijs van het tegendeel kan worden gegeven: enerzijds gegevens inzake facturatie, anderzijds medisch-administratieve documenten, met name de aanvragen van toiletten en forfaits, de kennisgevingen van de palliatieve zorgen en de aanvragen van de specifieke technische verpleegkundige verstrekkingen.

---

[1] Naar aanleiding van de opmerkingen die door de Informatieveiligheidsdienst van de Kruispuntbank van de Sociale Zekerheid werden gemaakt, heeft de Overeenkomstencommissie verpleegkundigen-verzekeringsinstellingen een nieuwe versie van bijlage II "*Oplossing MyCareNet: Technische principes van uitwisseling en reproductie van de gegevens*" van het protocol opgemaakt. Deze aangepaste bijlage II werd door deze commissie goedgekeurd op 29 juni 2010.

Het sectoraal comité en de Informatieveiligheidsdienst van de Kruispuntbank van de Sociale Zekerheid hebben het protocol onder andere onderzocht op basis van de criteria vermeld in artikel 9, 1° tot en met 5°, van het koninklijk besluit van 27 april 1999. De procedure in kwestie lijkt aan de voorvernoemde criteria te voldoen. Niettemin wenst het sectoraal comité een aantal aanbevelingen en suggesties te formuleren die kunnen bijdragen tot een grotere informatieveiligheid.

6. Technische principes

De gegevensuitwisseling verloopt via het MyCareNet-platform. Dit is een beveiligd netwerk tussen de zorgverstrekkers en de verzekeringsinstellingen, dat gebruik maakt van bepaalde diensten van het eHealth platform en het bestaande CareNet-netwerk. De informatieuitwisselingen via dit platform kunnen zowel *synchroon* (transactioneel) dan wel *asynchroon* (batch transfer – het antwoord op een vraag komt in uitgestelde tijd toe) zijn. De gegevens waarvoor via onderhavig protocol bewijskracht wordt gevraagd (facturatiebestanden en medisch-administratieve documenten) zullen momenteel enkel asynchroon verwerkt worden. De basisdienst eBox van het eHealth-platform wordt gebruikt om informatie te verstrekken betreffende het verloop van de verwerking (toestand van de verschillende informaties evenals hun historiek en de beschikbaarheid van de op te halen bestanden). De zorgverlener dient regelmatig de berichten in deze beveiligde elektronische mailbox op te vragen zodat hij op de hoogte is van de communicatie vanuit de verzekeringsinstellingen.

Voor het geïntegreerd beheer van gebruikers en toegangen (identificatie/authenticatie/autorisatie) met inbegrip van mandaten wordt gebruik gemaakt van basisdiensten zoals uitgewerkt door het eHealth-platform. Verschillende gevalideerde authentieke refertebestanden en controlesystemen bewaken de profielen van de potentiële gebruikers en aan de hand van die profielen kan dan bepaald worden of zij al dan niet toegang kunnen krijgen tot de toepassing in kwestie.

Het MyCareNet platform voorziet zowel in interacties *systeem-tot-systeem* (webservices) als in een *portaaltoepassing* (via www.mycarenet.be) voor de overdracht van gegevens. In beide gevallen dient de gebruiker zich eenduidig te authentificeren door middel van het authenticatiecertificaat op zijn elektronische identiteitskaart (eID). Zoals reeds eerder vermeld, wordt voor deze controle op de identiteit van de zorgverstrekker of zijn gemandateerde en voor de verificatie van zijn autorisaties beroep gedaan op gespecialiseerde basisdiensten van het eHealth-platform.

Na positieve authenticatie wordt een beveiligde sessie geopend. Conform de machtigingen nr. 07/003 van 9 januari 2007 en nr. 07/070 van 4 december 2007 is het communicatiekanaal[2] tussen de zorgverstrekker en MyCareNet geëncrypteerd: de beveiliging van deze verbinding is gebaseerd op SSL/TLS.

[2] In geval van een S2S (“systeem tot systeem” relatie): de verbinding tussen de toepassing van de softwareproducent en MyCarenet. In geval van de portaaltoepassing: de verbinding tussen browser op de pc van de gebruiker en MyCareNet.

De beveiliging op transportniveau gebeurt dus door het gebruik van HTTPS via *1-way SSL*. Dit zorgt voor een beveiligd communicatiekanaal. De afdeling sociale zekerheid van het sectoraal comité van de sociale zekerheid en van de gezondheid wenst op te merken dat gebruik van HTTPS via *2-way SSL* (zowel cliënt- als serverauthenticatie) sterk dient aanbevolen te worden. De documentatie van MyCareNet vermeldt dat alle *SSL cipher suites* ondersteund worden. Het is tevens sterk aangeraden deze lijst met cryptografische parameters restrictiever te maken teneinde aanvallen op het SSL protocol te vermijden.

De facturatiebestanden en de medisch-administratieve documenten uitgewisseld binnen MyCareNet (gegroepeerd per overdracht in een CPD (Care Provider Document)) worden voor integriteitdoelstellingen elektronisch getekend door middel van de eID, zowel in de "systeem naar systeem" als in de portaal gebruiksmode. Deze handtekening wordt globaal toegepast op het geheel van de documenten die overgemaakt worden in een CPD. De persoon die tekent kan de individuele zorgverlener zijn of de verantwoordelijke van de desbetreffende groepering van zorgverleners, alsook elke geautoriseerde MyCareNet gebruiker die door één van hen aangeduid is via het *user management* van eHealth of via een eHealth *mandaat*.

Om met de verzekeringsinstellingen te communiceren, wisselt MyCareNet berichten uit met een Client gateway via het CareNet netwerk. Bij de verzekeringsinstellingen bevindt zich een gateway Server. Deze gateways (*client* en *server*) nemen het digitaal ondertekenen en vercijferen van de informatie die verstuurd wordt via het netwerk op zich en dit met behulp van specifieke certificaten. De encryptie van deze verbinding tussen MyCareNet en de verzekeringsinstellingen gebeurt op basis van TDES (128 bit).

De uitwisseling van berichten tussen deze gateways verloopt volgens de technische principes zoals beschreven in de bijlagen van het CareNet-protocol, zoals opgemaakt op 19 april 2001 tussen de representatieve organisaties van verpleeginrichtingen en de verzekeringsinstellingen.

Het sectoraal comité wenst er aan te herinneren dat CareNet reeds gebruikt wordt voor de gegevensuitwisseling tussen ziekenhuizen en verzekeringsinstellingen conform de bij beraadslaging nr. 97/48 van 3 juli 1997 verleende machtiging en dat deze gegevens[3] in deze context bewijskracht genieten (zie advies nr. 01/011 van 11 december 2001). Hetzelfde CareNet-netwerk wordt nu ook gebruikt voor de gegevensuitwisseling tussen verpleegkundigen en de verzekeringsinstellingen, vanaf de MyCareNet-client GATEWAY en tot aan de server GATEWAY van de verzekeringsinstellingen.

Het is wenselijk de evolutie op vlak van cryptografische algoritmes op te volgen en te kiezen voor standaardalgoritmes. Hierbij wordt het gebruik van algoritmes zoals AES (met een minimum sleutelsterkte van 128-bits) sterk aanbevolen (in plaats van TDES). Het gebruik op middellange termijn van het hash-algoritme SHA1 wordt daarentegen afgeraden.

3 Bepaalde gegevens noodzakelijk voor de uitvoering van de verplichtingen van de verzekeringsinstellingen met betrekking to derdebetalersregeling en de correct uitvoering van de ziekenhuisopnames.

Met het oog op een onderlinge coherentie tussen de voorziene technische maatregelen, dient te worden overgegaan tot een precisering van de fysische en logische veiligheidsmaatregelen die van toepassing zijn op de PC's en de gateways clients/servers waarop, enerzijds, de berichten zullen worden verwerkt en, anderzijds, de publieke en privésleutels (*key management*) zullen worden bewaard. Een techniek van strenge authenticatie, in combinatie met fysische veiligheidsmaatregelen met beperkte toegang wordt aanbevolen.

7. Onweerlegbaarheid van verzenden en ontvangen

Bij MyCareNet worden de veiligheidsdiensten *data-integriteit* en *onweerlegbaarheid van oorsprong* gerealiseerd conform de bepalingen in de machtigingen nr. 07/003 van 9 januari 2007 en nr. 07/070 van 4 december 2007. De verzender (verpleegkundige of gemandateerde) ondertekent de documenten (in geval van meerder documenten, eigenlijk het geheel van documenten, dus niet elke document afzonderlijk) met behulp van zijn elektronische identiteitskaart: dit garandeert de oorsprong van het bericht en de niet-vervalsing ervan. Van zodra MyCareNet het bericht ontvangt, zal er door MyCareNet een auditnummer worden teruggestuurd naar de verzender. Gezien er geen eenduidige relatie bestaat tussen dit auditnummer en het verstuurde bericht wordt de dienst *onweerlegbaarheid van verzenden en ontvangen* niet geïmplementeerd. Het bericht wordt samen met het voorvermelde auditnummer door MyCareNet naar de verzekeringsinstellingen gestuurd via het bestaande CareNet. De link tussen het bericht en het gevormde auditnummer dient veilig bewaard te worden door zowel de verzender, het platform MyCareNet als de verzekeringsinstellingen.

Hierbij dient opgemerkt te worden dat bij CareNet (het protocol zoals opgemaakt op 19 april 2001) de veiligheidsdiensten *data-integriteit* en *onweerlegbaarheid van verzenden en ontvangen* wel degelijk worden gerealiseerd aan de hand van een combinatie van digitale handtekening en ontvangstbewijs (*return receipt*). Het onweerlegbaar vermoeden dat het bericht is ontvangen/verstuurd, wordt gewaarborgd door een verplichte ontvangstmelding die op zijn beurt wordt verstuurd met een elektronische handtekening door de verzekeringsinstelling: dit ontvangstbewijs bevat namelijk de handtekening van het verstuurde bericht en een ticketnummer, waarbij het geheel wordt ondertekend door de ontvanger (meer bepaald de GATEWAY server van de verzekeringsinstelling). De verzender van het bericht kan aan de hand van dit ontvangstbewijs verifiëren dat de bestemmeling het bericht wel degelijk ontvangen heeft waarbij de integriteit van het bericht gegarandeerd blijft.

8. Back Office-procedure en veiligheid

Gezien de heterogeniteit van de verschillende "back offices" is het moeilijk om een gemeenschappelijke archiveringsprocedure te omschrijven. Tevens is het moeilijk om de specifieke veiligheidsmaatregelen op alle eindpunten te specificeren (pc's zorgverleners, gateways servers verzekeringsinstellingen,…). Niettemin dienen afdoende veiligheidsmaatregelen te worden voorzien. Bij CareNet werd er een controle voorzien door middel van een checklist. Aan de hand van deze checklist werd nagegaan of de back office-

procedures beantwoorden aan de nodige (veiligheids)vereisten. Bij MyCareNet is een dergelijke controle (met checklist) niet voorzien.

Het is wenselijk dat voor de eindpunten bij MyCareNet de volgende aanbevelingen worden nageleefd:

- Conformiteit met de verschillende vereisten door middel van een checklist, naar analogie met CareNet (veiligheidsvereisten, beschrijving van archiveringsprocedure,…).
- De PC's van de zorgverlener (of gemandateerde) dienen te voldoen aan minimale veiligheidsvereisten (antivirus, firewall, patch management,…). Bijvoorbeeld de veiligheidsmaatregelen die opgenomen zijn in de door de werkgroep Informatieveiligheid opgestelde policies (zie verder).
- Er wordt voorgesteld om op geregelde tijdstippen en volgens door het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering nader te bepalen modaliteiten een audit met betrekking tot de archiveringsprocedure te organiseren. Een dergelijke – door een onpartijdige instantie uit te voeren – audit kan voor de veiligheidsconsulent immers een hulpmiddel vormen.

Het sectoraal comité wijst op de noodzaak voor de betrokken instellingen en entiteiten om, wanneer gebruik gemaakt wordt van een werkstation (zowel vaste pc als laptop) de regels toe te passen die door de werkgroep Informatieveiligheid in de policy "*Beleid voor de beveiliging van werkstations*" geformuleerd werden.

Het sectoraal comité wijst tevens op de noodzaak voor de betrokken instellingen en entiteiten om bij het gebruik van een laptop de regels toe te passen die door de werkgroep Informatieveiligheid geformuleerd werden in de policy "*Veiligheidsbeleid Draagbare PC*".

Ook wordt de aandacht gevestigd op de noodzaak voor het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering om de Kruispuntbank van Sociale Zekerheid en het sectoraal comité van de sociale zekerheid en van de gezondheid in te lichten en documentatie te verschaffen in geval van evolutie naar nieuwe technieken of procedures. Het zou aangewezen zijn indien het sectoraal comité dit protocol (op langere termijn) aan een nieuw onderzoek zou kunnen onderwerpen in functie van de aangebrachte wijzigingen.

Met betrekking tot artikel 6 van het voorgelegde protocol dient overgegaan te worden tot een precisering van de te archiveren gegevens bij zowel de verzekeringsinstellingen, het MyCareNet platform als de informaticasystemen van de prestatieverleners.

9. Loggings

In geval van interacties systeem-tot-systeem gebruikt de verpleegkundige een toepassing van een softwareproducent. Naast de loggings door MyCareNet en de verzekeringsinstellingen wordt ook aan de softwareproducenten van de toepassing gevraagd om te zorgen voor een systeem van loggings. De toegang tot de loggings dient te worden beperkt tot de veiligheidsconsulenten van de bij de toepassing betrokken instellingen van sociale zekerheid, in opdracht van het sectoraal comité van de sociale

zekerheid en van de gezondheid of van de leidinggevenden van de betrokken instellingen van sociale zekerheid. Bij de toegang tot de loggings dient eveneens te worden voorzien in een degelijk systeem van identificatie en authenticatie, bijvoorbeeld aan de hand van de elektronische identiteitskaart. Voor de verzekeringsinstellingen en MyCareNet zijn er veiligheidsconsulenten aangesteld. De loggings van toepassing(en) van de softwareproducenten dienen tevens beschikbaar gesteld te worden van het sectoraal comité.

De veiligheidsconsulenten van de betrokken instellingen of entiteiten zien toe op het bestaan van logbestanden en de correcte bewaring ervan, in overeenstemming met de machtigingen van het sectoraal comité van de sociale zekerheid en van de gezondheid (beraadslagingen nr. 07/003 van 9 januari 2007 en nr. 07/070 van 4 december 2007).

De loggings dienen het sectoraal comité van de sociale zekerheid en van de gezondheid in staat te stellen zijn controleopdracht te vervullen. Ze dienen minstens te worden bijgehouden gedurende een periode van tien jaren.

Om deze redenen, verleent

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

een gunstig advies op voorwaarde dat de onder punt 8 vermelde aanbevelingen worden geïmplementeerd binnen een termijn van zes maanden. Het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering dient het sectoraal comité van de sociale zekerheid en van de gezondheid daarover in te lichten.

Aldus dienen voor de eindpunten bij MyCareNet de volgende aanbevelingen te worden nageleefd:

- Conformiteit met de verschillende vereisten door middel van een checklist, naar analogie met CareNet (veiligheidsvereisten, beschrijving van archiveringsprocedure,…).

- De PC's van de zorgverlener (of gemandateerde) dienen te voldoen aan minimale veiligheidsvereisten (antivirus, firewall, patch management,…). Bijvoorbeeld de veiligheidsmaatregelen die opgenomen zijn in de door de werkgroep Informatieveiligheid opgestelde policies.

- Er wordt voorgesteld om op geregelde tijdstippen en volgens door het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering nader te bepalen modaliteiten een audit met betrekking tot de archiveringsprocedure door een onpartijdige instantie te organiseren.

Yves ROGER
Voorzitter