RIZIV
Rijksinstituut voor Ziekte- en Invaliditeitsverzekering

OMZENDBRIEF AAN DE ZIEKENHUIZEN
OMZ. 2003/4

DIENST VOOR GENEESKUNDIGE VERVERZORGING

Correspondent: Dr Yves Beterams

Tel.: 02/739.77.86 **Fax:** 02/739.77.11
E-mail:
Onze referte: 1300/YB/omz-2003-4 **Brussel,** 17-04-2003

Gegevensuitwisseling via CareNet en het Protocol Bewijskracht Verordening van 17 december 2001 (BS 11 april 2002).

Mevrouw de Directrice,
Mijnheer de Directeur,

In aansluiting op de omzendbrief aan de ziekenhuizen (omz. 2002/3) van 18 juni 2002 worden de verpleeginrichtingen die de gegevens, vermeld op de formulieren 721bis – 723 – 725 en 727 via Carenet overmaken, ondermeer herinnerd aan de procedures die zijn bepaald in artikel 5 van het protocol van 19 april 2001 en de bijlage "Back Office-procedure" bij datzelfde protocol.

Hier wordt het protocol bedoeld van 19 april 2001 gesloten tussen de representatieve organisaties van de verpleeginrichtingen en de verzekeringsinstellingen, houdende de voorwaarden en modaliteiten volgens welke bewijskracht kan worden gegeven tot het bewijs van het tegendeel aan gegevens die worden opgeslagen of bewaard door middel van een elektronische, fotografische, optische of elke andere techniek of medegedeeld op een ander 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.

Verdere informatie hieromtrent vindt u in de map "Zorgverleners – Carenet " op de website van het Riziv **http://www.riziv.fgov.be**.

Hoogachtend
De leidend ambtenaar

F. PRAET
Directeur-generaal.

Tervurenlaan 211 · B-1150 Brussel Tel.: 02 739 71 11 · Fax: 02 739 72 91
Openingsuren van de kantoren: **van 9 tot 12 uur en van 13 tot 16 uur. Afspraak mogelijk.**

**Protocol, gesloten op 19 april 2001 tussen de representatieve organisaties van de verpleeginrichtingen en de verzekeringsinstellingen,
houdende de voorwaarden en modaliteiten volgens welke bewijskracht kan worden gegeven tot het bewijs van het tegendeel aan gegevens die worden opgeslagen of bewaard door middel van een elektronische, fotografische, optische of elke andere techniek of medegedeeld 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**

Kennisgeving ziekenhuisverpleging en betalingsverbintenis
Aanvraag om verlenging van ziekenhuisverpleging
Gegevens inzake het akkoord voor verdere tenlasteneming
van de ziekenhuisverpleging
Mededeling van wijziging van dienst
Kennisgeving van einde ziekenhuisverpleging
Gegevens inzake de identiteit en de verzekerbaarheid van de rechthebbende

Art 5. Vooraleer in uitvoering van het vorengenoemd koninklijk besluit van 27 april 1999 en van dit protocol aan de gegevens die door een ziekenhuis of door een verzekeringsinstelling worden overgemaakt bewijskracht kan worden gegeven moeten deze, éénmalig, aan de Administrateur generaal van het Riziv, aan de hand van een checklist (**zie bijlage 3**), aantonen dat zij voldoen aan de bepalingen die zijn opgenomen in dit protocol en zijn bijlagen. De ontvangst hiervan zal enerzijds worden bevestigd aan het betrokken ziekenhuis of aan de verzekeringsinstelling, en zal anderzijds bekend gemaakt worden in een omzendbrief aan de verzekeringsinstellingen.

Bijlage 3 Back Office-procedure

Inleiding

Document dat als bijlage bij het CARENET-protocol van het RIZIV wordt gevoegd, en dat bestemd is om de noodzakelijke voorwaarden vast te leggen om bewijskracht te verlenen (en te handhaven) aan de via CARENET verstuurde documenten en waarin de principes zijn vermeld die voor de archivering van de gegevens door de verschillende CARENET-actoren moeten worden in acht genomen.

De cryptografische technieken die door de CARENET GATEWAY bij de uitwisselingen gebruikt worden, waarborgen de vertrouwelijkheid, de authentificatie, de integriteit en de niet-verwerping van de verstuurde gegevens. Om hun bewijskracht in de loop der jaren te handhaven en ze als te bewijs te kunnen gebruiken, moeten deze beveiligingselementen veilig worden bewaard.

Daar de back offices van nature verschillen, is het onmogelijk om nauwkeurig een gemeenschappelijke procedure te omschrijven. In dit document worden de algemene regels vastgelegd die bij de archivering van de via CARENET uitgewisselde gegevens moeten worden nageleefd, opdat aan deze gegevens bewijskracht kan worden verleend (en kan worden gehandhaafd). De volledige beschrijving van de procedures valt onder de verantwoordelijkheid van elk van de CARENET-actoren.

Procedures van toepassing bij geschillen

Betwisting door de zender:

- Opzoeken van het nummer van de BUFFER die het bericht in kwestie bevat (of waarin dit ontbreekt)
- Deze BUFFER opzoeken en de handtekening op het CARENET-bericht opnieuw berekenen
- De handtekening vergelijken met het ondertekend bericht van ontvangst van de ontvanger

Betwisting door de ontvanger:

- Opzoeken van het nummer van de BUFFER die het bericht in kwestie bevat (of waarin dit ontbreekt)
- Deze BUFFER opzoeken en de handtekening op het CARENET-bericht opnieuw berekenen
- De handtekening van de zender controleren

Vereiste stukken die moeten worden bewaard en die bij geschillen moeten worden voorgelegd

De zender van een CARENET-bericht moet bewaren:

- Het volledige verstuurde bericht
- Het bericht van ontvangst van het verstuurde bericht
- De log-bestanden message en error

- Om het onderzoek te vergemakkelijken, zou ook de link tussen het bericht en het gevormde BUFFER-nummer moeten worden bewaard.
- De gegevens die betrekking hebben op de controle van de handtekening van elk bericht (digitaal certificaat van de ondertekenaar, de certificaatketting, de lijst van herroeping van de certificaten op het moment van de controle)
- De garantie dat al deze gegevens authentiek en waarachtig zijn

De ontvanger van een CARENET-bericht moet bewaren:

- Het volledige ontvangen bericht
- Het verstuurde bericht van ontvangst
- De log-bestanden message en error
- Om het onderzoek te vergemakkelijken, zou ook de link tussen het bericht en het ontvangen BUFFER-nummer moeten worden bewaard.
- De gegevens die betrekking hebben op de controle van de handtekening van elk bericht (digitaal certificaat van de ondertekenaar, de certificaatketting, de lijst van herroeping van de certificaten op het moment van de controle)
- De garantie dat al deze gegevens authentiek en waarachtig zijn

Functionele beschrijving van de procedures die door de verschillende actoren moeten worden overeengekomen om de opslag, de bewaring en de reproductie van de uitgewisselde gegevens te verzekeren.

1. Beschrijving van de te archiveren gegevens

- Alle uitgewisselde berichten
- De lijst van de uitgewisselde BUFFERS, samen met hun HEADER
- Het bewaren van de link tussen het bericht en de BUFFER waarin het is verstuurd, is verplicht. Met deze link kan de BUFFER waarin een bericht verstuurd werd, bepaald worden, en kan de BUFFER met al zijn berichten opnieuw worden samengesteld.
- De logging van de berichten van de GATEWAY, die de handtekeningen van de uitgewisselde berichten en de referenties van de BUFFERS bevat
- De logging van de fouten van de GATEWAY
- De gegevens die betrekking hebben op de controle van de handtekening van elk bericht (digitaal certificaat van de ondertekenaar, de certificaatketting, de lijst van herroeping van de certificaten op het moment van de controle)
- De garantie dat al deze gegevens authentiek en waarachtig zijn

2. Beschrijving van de archiveringsprocedure

Dagelijks worden alle in punt 1 vermelde bestanden in twee verschillende exemplaren opgeslagen op een niet-vluchtige drager. Deze bewaarde bestanden mogen aan de eerder opgeslagen bestanden worden toegevoegd, maar moeten achteraf ervan kunnen worden losgemaakt.

3. Beschrijving van de procedures voor bewaring van de archieven

De archieven worden zo opgeslagen dat ze achteraf niet meer kunnen worden gewijzigd of dat elke achteraf aangebrachte wijziging op te sporen is. De archieven worden gekopieerd en bewaard op fysiek verschillende plaatsen om te voorkomen dat ze door een ongeval allemaal tegelijk zouden worden vernietigd. Deze archieven worden tegen fysieke aantastingen (brand, overstroming) beschermd en, om de vertrouwelijke aard ervan te vrijwaren, krijgen uitsluitend vooraf aangewezen personen toegang ertoe.

4. Beschrijving van de procedure voor opzoekingen in het archief en publicatie van de archieven

Toegang tot de gegevens kan worden verkregen door onderstaande opzoekingscriteria, apart of gecombineerd, in te voeren: INSZ, datum van verzending, datum van ontvangst, nummer van het bericht, type bericht, nummer van de mailbox, instelling, bestand. Behoudens toevallige incidenten en op voorwaarde dat de opzoeking tijdens de normale kantooruren plaatsvindt, zouden de opzoekingen binnen een termijn van 4 uren na de aanvraag resultaat moeten opleveren. Het resultaat van de opzoekingen wordt op een scherm weergegeven en ze moeten geheel of gedeeltelijk kunnen worden afgedrukt.

5. Beschrijving van de gebruikte informatiemiddelen, software en hardware

De gebruikte hardware, software en dragers moeten algemeen verspreid zijn en van dien aard zijn dat de toepassingen even lang bewaard blijven als de maximale bewaartermijn van de gegevens. Als zou blijken dat de gebruikte techniek niet meer door de leverancier wordt aangeboden, zou de instelling ervoor moeten zorgen dat de informatie op een nieuwe drager wordt opgeslagen.

Opmerkingen

- In elke fase van de procedure moet de exacte, duurzame en volledige reproductie van de informatie worden gegarandeerd en moet voor een systematische en volledige opslag van de gegevens worden gezorgd.
- De gearchiveerde gegevens moeten gedurende een periode van 10 jaar bewaard, geklasseerd en tegen elke aantasting worden beschermd.
- De veiligheidsmaatregelen die zijn genomen om de vertrouwelijke aard van de gegevens te vrijwaren, moeten worden vermeld.
- Voor elke fase moet een logboek worden bijgehouden waarin de volgende gegevens worden genoteerd :
  - de identiteit van de persoon die verantwoordelijk is voor de verwerking;
  - de identiteit van de persoon die de verwerking heeft uitgevoerd;
  - de aard van de verwerkte informatie;
  - datum, uur en plaats van de verwerking;
  - eventuele vastgestelde storingen.

- Alle gebruikte procedures, hardware en software moeten gedetailleerd worden beschreven in een dossier dat regelmatig wordt bijgewerkt en waarvan een exemplaar aan de veiligheidsconsulent van de instelling wordt overhandigd en een tweede ter beschikking van de controlediensten van het RIZIV wordt gesteld.

Rol van de veiligheidsconsulent

De veiligheidsconsulent adviseert, op eigen initiatief of op verzoek, de persoon die instaat voor het dagelijks beheer van de instelling. Hij is belast met het verzamelen, bijwerken en verdelen van de nodige documentatie. Hij waakt ook over de correcte toepassing van de binnen de instelling overeengekomen procedures. Hij brengt jaarlijks verslag uit over de daadwerkelijke naleving van de procedures. Elke vastgestelde tekortkoming moet te allen tijde onmiddellijk aan de directie van de instelling worden gemeld. De adviezen en verslagen moeten schriftelijk worden meegedeeld en met redenen worden omkleed.

Checklist

Checklist om na te gaan of in het archiveringsdossier van de instelling is voldaan aan de verschillende vereisten waaraan de back office-procedures moeten beantwoorden. In die checklist wordt dus de minimale informatie vermeld die het dossier moet bevatten om te beantwoorden aan de nodige vereisten om bewijskracht aan de elektronische documenten te geven.

ALGEMEEN	
	Benaming van de instelling
	Naam van het document
	Verantwoordelijke opsteller
	Opvolging van de versies en bijwerkingen
	Datum van afdruk
	Plaats waar gestockeerd of ter beschikking gehouden wordt
	Naam van de veiligheidsconsulent
	Datum van de laatste afgifte aan de veiligheidsconsulent
	Lijst van de personen die in de verschillende etappes toegang hebben tot de gegevens
ETAPPE 1: Systematische en volledige registratie van de gegevens	
Aard en onderwerp van de informatie waarop de verwerking betrekking heeft	Alle uitgewisselde berichten
	De lijst van de uitgewisselde BUFFERS samen met hun HEADER
	Link tussen elk bericht en de BUFFER waarin het is verstuurd. Die link moet toelaten de BUFFER, waarin een bericht is verstuurd, te bepalen en de BUFFER weer samen te stellen met al zijn berichten
	De logging van de berichten van de GATEWAY met als inhoud de handtekeningen van de uitgewisselde berichten alsook de referenties van de BUFFERS
	De logging van de fouten van de GATEWAY
	De gegevens die betrekking hebben op de controle van de handtekening van elk bericht (digitaal certificaat van de ondertekenaar, certificaatketting, de lijst van herroeping van de certificaten op het moment van de controle
Beschrijving van de procedure van systematische en volledige registratie van de gegevens	De omgeving
	De stromen
	De periodiciteit van de verrichtingen
	De controle van de kwaliteit

	Reactie in geval van incidenten
	Beschrijving van de middelen en karakteristieken van de gebruikte softwares
	Beschrijving van de middelen en karakteristieken van de gebruikte hardware
	Veiligheidsmaatregelen voor de vertrouwelijkheid van de gegevens
Gegevens met betrekking tot de verwerking die moeten bewaard blijven	Verantwoordelijke van het logboek, plaats van raadpleging ervan of plaats van stockering
	Identiteit van de verantwoordelijke van de verwerking
	Identiteit van de persoon die de verwerking heeft uitgevoerd
	Aard en onderwerp van de informatie met betrekking tot de verwerking
	Datum en plaats van de verrichting
	Eventuele stoornissen
ETAPPE 2: Bewaren van de systematisch geklasseerde en tegen elke wijziging beveiligde gegevens	
Beschrijving van de procedure die de bewaring van de systematisch geklasseerde en tegen elke wijziging beveiligde gegevens beschrijft	Plaats van stockering
	Beschrijving van de organisatorische en technische maatregelen die de onveranderlijkheid van de bewaarde en gestockeerde gegevens waarborgen
	Beschrijving van de procedures voor de periodieke bewaring van de back-up van bewaarde gegevens met garantie van hun mogelijke restitutie
	Beschrijving van de methode van het klassement
	Beschrijving van de manieren van bescherming tegen o.a. kwaadwilligheid, brand, overstromingen
	De controle op de toegang van de gegevens
	Reactie in geval van incidenten
	Voorziene veiligheidsmaatregelen teneinde het vertrouwelijke karakter van de gegevens te beschermen
Gegevens met betrekking tot de verwerking die moeten bewaard blijven	Verantwoordelijke van het logboek, plaats van raadpleging ervan of plaats van stockering
	Identiteit van de verantwoordelijke van de verwerking
	Identiteit van de persoon die de verwerking heeft uitgevoerd
	Aard en onderwerp van de informatie waarop de verwerking betrekking heeft
	Datum en plaats van de verrichting
	Eventuele stoornissen
ETAPPE 3: Getrouwe, duurzame en volledige reproductie van de informatie	
Beschrijving van de procedure die de trouwe, duurzame en volledige weergave van de informatie waarborgt	De omgeving
	De stromen
	Beschrijving van de toegangsmiddelen en de opzoekingcriteria van de gegevens
	De controle van de kwaliteit
	Reactie in geval van incidenten
	Beschrijving van de middelen en karakteristieken van de gebruikte softwares
	Beschrijving van de middelen en karakteristieken van de gebruikte hardware alsook van de gecreëerde outputs

	Voorziene veiligheidsmaatregelen teneinde het vertrouwelijke karakter van de gegevens te beschermen
Logboek	Verantwoordelijke van het logboek, plaats van raadpleging hiervan of plaats van stockering
	Identiteit van de verantwoordelijke van de verwerking
	Identiteit van de persoon die de verwerking uitgevoerd heeft
	Aard en onderwerp van de informatie waarop de verwerking betrekking heeft
	Datum en plaats van de verrichting
	Eventuele stoornissen