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

SCSZ/09/121

ADVIES NR 09/22 VAN 6 OKTOBER 2009 BETREFFENDE DE AANVRAAG VAN HET OZ ONAFHANKELIJK ZIEKENFONDS VOOR HET VERKRIJGEN VAN EEN MINISTERIËLE ERKENNING VOOR EEN ELEKTRONISCH ARCHIVERINGSSYSTEEM IN TOEPASSING VAN HET KONINKLIJK BESLUIT VAN 22 MAART 1993 BETREFFENDE DE BEWIJSKRACHT

Gelet op de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid, inzonderheid op artikel 15, tweede lid;

Gelet op de aanvraag van het OZ Onafhankelijk Ziekenfonds van 21 augustus 2009;

Gelet op het auditoraatsrapport van de Kruispuntbank van 30 september 2009;

Gelet op het verslag van de heer Yves Roger.

A. CONTEXT EN ONDERWERP VAN DE AANVRAAG

1.1. Het OZ Onafhankelijk Ziekenfonds (***OZ***[1]) heeft op 21 augustus 2009 een erkenningsaanvraag ingediend bij het Sectoraal Comité van de Sociale Zekerheid.

Deze aanvraag heeft het verkrijgen van een ministeriële erkenning voor haar procedures in het kader van de toepassing van het koninklijk besluit van 22 maart 1993 betreffende de bewijskracht, ter zake van de sociale zekerheid, van de door instellingen van sociale zekerheid opgeslagen, bewaarde of weergegeven informatiegegevens tot doel.

[1] De Landsbond van de Onafhankelijke Ziekenfondsen verenigt zeven ziekenfondsen: Euromut, Partena Ziekenfonds & Partners, Onafhankelijk Ziekenfonds Securex, **het OZ Onafhankelijk Ziekenfonds**, Partenamut Mutualité Libre, de Mutualité Professionnelle et Libre de la Région wallonne en de Freie Krankenkasse.

B. BEHANDELING VAN DE AANVRAAG

2. De evaluatie van de procedures die werden ingediend voor het verkrijgen van de ministeriële erkenning is opgesplitst volgens de technische voorwaarden van artikel 3 van het koninklijk besluit van 22 maart 1993.

Deze voorwaarden werden punt voor punt besproken in het dossier van ***OZ***.

Het auditoraatsrapport is het resultaat van een samenwerking met de verantwoordelijken en de interne en externe technici van de betrokken instelling.

Deze samenwerking omvatte verschillende stappen, namelijk:

- ✓ een informatievergadering op de Kruispuntbank van de Sociale Zekerheid om het ***OZ*** in te lichten over de noodzakelijke inhoud voor de goedkeuring van het dossier 'bewijskracht' (29 april 2008);
- ✓ de overmaking door de instelling van een eerste versie van zijn dossier aan de informatieveiligheidsdienst van de Kruispuntbank van de Sociale Zekerheid (3 februari 2009);
- ✓ een werkvergadering op 25 maart 2009 besteed aan een kritische analyse van het dossier;
- ✓ de overmaking door de instelling van een nieuwe versie van zijn dossier aan de informatieveiligheidsdienst van de Kruispuntbank van de Sociale Zekerheid (24 april 2009);
- ✓ het opstellen door de veiligheidsdienst van de Kruispuntbank van een reeks bijkomende vragen over verschillende aspecten van de geïmplementeerde procedure;
- ✓ een bezoek (audit) van de informatieveiligheidsdienst van de Kruispuntbank aan de site van het ***OZ*** waar een demonstratie en een vragenronde met de betrokken actoren plaatsvonden (18 juni en 1 juli 2009);
- ✓ er werden tevens e-mails uitgewisseld met het oog op een kritische analyse van het dossier en om een aantal details te preciseren;
- ✓ het opstellen door het ***OZ*** van een dossier ten behoeve van het Sectoraal Comité van de Sociale Zekerheid.

Het voorstel omschrijft nauwkeurig de procedure.

2.1. Het door ***OZ*** ingediend dossier bevat een beschrijving van de geïmplementeerde procedures voor de registratie en het bewaren van de informatiegegevens aan de hand van een beveiligd elektronisch archiveringssysteem**,** en de weergave ervan op een leesbare drager.

In het voorgestelde dossier worden de mechanismen, de controles en de tussenkomende partijen nauwkeurig omschreven.

De aangewende technologie waarborgt een getrouwe, duurzame en volledige weergave van de informatie.

2.2. Het door ***OZ*** toegelicht dossier heeft ons ertoe aangezet na te gaan of de beschreven oplossing inzake elektronisch documentenbeheer de bepalingen van § 2 van artikel 3 van het koninklijk besluit van 22 maart 1993 wel naleeft.

Hiertoe hebben we bijzondere aandacht besteed aan de volgende aspecten:

- ✓ de componenten van de technische oplossingen (technische architectuur en software);
- ✓ het circuit van verwerking en scanning van de betrokken dragers;
- ✓ het automatische en manuele controlepunt volgens de fases van het proces;
- ✓ de overmaking van de elektronische documenten in het document management systeem;
- ✓ de formaten van de bestanden en de overeenstemming ervan met de archiveringsstandaarden die de duurzaamheid van de geregistreerde gegevens garandeert;
- ✓ het beheer van de incidenten, de fouten en de mechanismen van eventuele overname of verwerping van de informatie;
- ✓ de instructies voor de aanwending van de oplossing;
- ✓ afhandeling van het scanproces: de behandeling van een blanco bladzijde tijdens de scanning, de behandeling van documenten met een niet-standaardformaat, … ;
- ✓ het voorzien van onderhoudscontracten m.b.t. de geïnstalleerde soft- en hardware;
- ✓ de aanwezigheid van een interne supportafdeling;
- ✓ de maatregelen/controles die waarborgen dat er aan de opgeslagen informatiegegevens geen wijzigingen worden aangebracht;
- ✓ de controle van de kwaliteit en de kwantiteit.

De informatie wordt systematisch geregistreerd.

2.3. In het dossier van de ***OZ*** worden de procedures beschreven met betrekking tot:

- ✓ de indexering van de documenten;
- ✓ de onmogelijkheid om gescande documenten te wijzigen of te verliezen of ze meermaals te registreren;
- ✓ de wijze van registratie en het geldigheidsmechanisme van de indexen;
- ✓ het opnieuw samenstellen van de indexen;
- ✓ de toegangsbeperking tot de indexen;
- ✓ de uitvoering van kwaliteits- en kwantiteitscontrole bij het inscannen van documenten.

Tijdens de demonstratie hebben we deze verschillende aspecten kunnen controleren.

De verwerkte informatie wordt op een zorgvuldige manier bewaard, systematisch gerangschikt en beschermd tegen elke vervalsing.

2.4. De ***OZ*** heeft onder meer de volgende maatregelen geïmplementeerd:

- ✓ afdoende maatregelen werden genomen om de continuïteit van de dienstverlening en de reconstructie ingeval van een belangrijk incident te kunnen waarborgen (o.a redundante SAN-infrastructuur);

- ✓ met betrekking tot het back-upsysteem zijn er duidelijke uitvoeringsregels volgens een vooraf bepaalde planning en rotaties van dragers in functie van de planning voorzien; deze procedures zijn in het globale back-upsysteem van de instelling opgenomen;
- ✓ afdoende disaster recovery maatregelen werden genomen en uitgetest;
- ✓ afdoende maatregelen werden getroffen m.b.t. fysieke beveiliging van gebouw, apparatuur en back-ups tegen natuurlijke risico's zoals brand, wateroverlast, acclimatisatie- en elektriciteitsproblemen;
- ✓ voor de fysieke toegangscontrole wordt gebruik gemaakt van een centraal beheerd badgesysteem;
- ✓ de periode van retentie en bewaring van de dragers is vastgelegd;
- ✓ de logische toegangsbeveiliging berust op verschillende methodes naar gelang het beoogde informatiesysteem en de aan de gebruikers toevertrouwde activiteiten; de toegangsrechten worden bepaald door middel van RBAC (role based access control);
- ✓ de aansluiting op het informatiesysteem is mogelijk via afdoende beveiligde werkposten binnen de instelling en via een beveiligde toegang op afstand (VPN en certificaat) in het kader van teleworking;
- ✓ de betrokken toepassingen en software worden onderhouden d.m.v. een patchbeleid dat mogelijke zwakheden in de geïmplementeerde oplossing dicht. Testen, acceptatie en release van nieuwe versies van een component van de oplossing lopen in overeenstemming met het standaard OZ release management proces. De procedures en voorbeelden van documentatie m.b.t. release management waren ter inzage beschikbaar tijdens de audit van de Kruispuntbank van Sociale Zekerheid;
- ✓ als instelling van het secundaire netwerk rond de Kruispuntbank van de Sociale Zekerheid dient het OZ de minimale veiligheidsnormen na te leven.

Tijdens het plaatsbezoek was alle nodige documentatie (handleidingen, disaster recovery plan, VPN security policy, …) ter inzage beschikbaar.

Bewaren van de volgende gegevens met betrekking tot de verwerking van de informatie: identiteit van de verantwoordelijke voor de verwerking evenals van diegene die ze heeft uitgevoerd, de aard en het onderwerp van de informatie waarop de verwerking betrekking heeft, de datum en de plaats van de verwerking, de eventuele storingen die zijn vastgesteld tijdens de verwerking.

2.5. De ***OZ*** heeft zijn systeem uitgerust met:

- ✓ diverse automatische loggings waardoor de gebeurtenissen van de verschillende componenten in ieder stadium van het proces kunnen worden bewaard; de toegang tot deze informatie gebeurt volgens een beveiligd proces; de loggings worden mee in de standaard back-upprocedures van de instelling geïntegreerd.

Om deze redenen, verleent

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

een gunstig advies.

Yves ROGER
Voorzitter