Checklist

Aan de hand van onderstaande checklist moet de prestatieverlener of de VI nagaan of aan alle procedures in het archiveringsdossier van de prestatieverlener of de VI is voldaan alsook aan de verschillende vereisten waaraan de BackOffice procedures moeten beantwoorden.
In deze 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.

Deze checklist bevat eveneens de informatie waaraan de beveiliging van het informaticamateriaal van de prestatieverlener (of zijn volmachthouder) moet voldoen.

Het ingevulde document moet beschikbaar zijn in geval van audit aangaande de archiveringsprocedure bij de prestatieverlener of de VI.

ALGEMEEN	
	Benaming, adres en RIZIV nummer van de instelling Benaming en adres van de VI
	Verantwoordelijke opsteller (Naam, voornaam en functie)
	Datum van afdruk

<table>
<tr><td colspan="2">ARCHIVERING</td></tr>
<tr><td colspan="2">STAP 1 : SYSTEMATISCHE EN VOLLEDIGE ARCHIVERING VAN ALLE UITWISSELINGSACTIVITEITEN MET HET PLATFORM MYCARENET

Terminologie :
Archivering = opslag van gegevens gedurende 10 jaar</td></tr>
<tr><td rowspan="3">Lijst van gegevens die moeten gearchiveerd worden bij de prestatie-verlener of de VI.

Dit betreft enkel de uitwisselingen facturatie en medisch-administratieve berichten.</td><td>Lijst van alle uitgewisselde berichten is beschikbaar : JA / NEEN</td></tr>
<tr><td>De logging van de fouten is beschikbaar : JA / NEEN</td></tr>
<tr><td>De gegevens die betrekking hebben op de controle van de handtekening gedaan op het geheel van de uitgewisselde berichten zijn beschikbaar (digitaal certificaat van de ondertekenaar) : JA / NEEN</td></tr>
<tr><td colspan="2">STAP 2 : Bewaren van de archieven (zoals opgemaakt in etappe 1)</td></tr>
<tr><td rowspan="3">Beschrijving van de procedure voor het bewaren van de archieven waarbij elke wijziging onmogelijk is</td><td>Plaats van stockeren van de archieven (“waar bevinden zich de archieven?”) :</td></tr>
<tr><td>De archieven zijn gedupliceerd en bewaard in verschillende fysieke locaties : JA / NEEN</td></tr>
<tr><td>Beschermingsmaatregelen zijn genomen tegen o.a. kwaadwilligheid, brand, overstromingen : JA / NEEN</td></tr>
<tr><td colspan="2">STAP 3 : Getrouwe, duurzame en volledige reproductie van de archieven</td></tr>
<tr><td rowspan="2">Beschrijving van de procedure die de getrouwe, duurzame en volledige weergave van de informatie waarborgt</td><td>De prestatieverlener of VI kent de procedure die de getrouwe reproductie van de archieven toelaat : JA / NEEN</td></tr>
<tr><td>De toegang tot de archieven kan gebeuren op basis van verschillende opzoekingcriteria : JA / NEEN</td></tr>
</table>

INFORMATIE BETREFFENDE DE VEILIGHEIDSVOORWAARDEN WAARAAN DE WERKPOSTEN VAN DE PRESTATIEVERLENER (OF ZIJN VOLMACHTHOUDER) MOETEN VOLDOEN	
Firewall	De interne firewall moet geactiveerd worden. Deze firewall moet doorlopend geactualiseerd worden.
	Enkel de poorten open laten die nodig zijn voor het uitvoeren van de professionele taken.
	Een onderscheid maken tussen connecties nodig voor het interne netwerk en externe connecties.
Anti-virus	Laat de anti-malware software regelmatig een volledige systeemscan uitvoeren (alle bestanden, ook van de startup files, bios, boot records).
	Maak gebruik van de real-time functies aanwezig in de anti-malware programma's.
	De anti-malware software moet regelmatig automatisch bijgewerkt worden.
Beheer van de patches	Veiligheidsupdates moeten eerst getest worden alvorens ze in productie uit te voeren.
	Na de testfase moeten de patches zo vlug mogelijk automatisch uitgevoerd worden op elk werkstation dat zich connecteert op het domein.
	Nieuwe werkstations mogen niet op het netwerk geïnstalleerd worden totdat deze systemen op een aanvaardbaar niveau van patching gebracht zijn.
	Voor de installatiefrequentie van de veiligheidsupdates moet een gezond evenwicht gevonden worden tussen de veiligheidsnoden en de operationele doelstellingen. Voor updates die door erkende instellingen als dringend worden aangegeven moeten onmiddellijk de gepaste maatregelen genomen worden.
	Een regelmatige communicatie tussen de dienst verantwoordelijk voor het patching beheer van de werkstations en de netwerkdienst moet georganiseerd worden. Het doel hiervan is om veiligheidsincidenten die door de netwerkdienst gedetecteerd worden te evalueren in het kader van het patching beheer en om indien nodig onmiddellijk maatregelen te treffen.

Extra informatie is beschikbaar bij de Kruispuntbank van de Sociale Zekerheid :

- « Beleid voor de beveiliging van werkstations » bij het gebruik van een computer (vast of draagbaar).
- « Veiligheidsbeleid Draagbare PC» bij het gebruik van een draagbare computer.