Check liste

Check liste destinée à vérifier que les différentes exigences auxquelles les procédures back office doivent répondre sont reprises dans le dossier d'archivage des prestataires ou de l'OA. Elle reprend donc les informations minimums que doit contenir ce dossier pour répondre aux conditions nécessaires afin de donner force probante aux documents électroniques.

Cette check liste reprend également des informations relatives à la sécurité auxquelles les ordinateurs du dispensateur de soins (ou de son mandataire) doivent répondre.

Le document complété doit être disponible en cas d'audit relatif à la procédure d'archivage chez le prestataire ou l'OA.

GENERALITES	
	Dénomination, adresse et numéro INAMI du prestataire Dénomination et adresse de l'OA
	Auteur responsable (Nom, prénom et fonction)
	Date d'impression

ARCHIVAGE	
ETAPE 1 : ARCHIVAGE SYSTEMATIQUE ET COMPLET DE TOUTES LES ACTIVITES D'ECHANGE AVEC LA PLATEFORME MYCARENET Terminologie : **archivage =** stockage des données pendant 10 ans.	
Liste des données à archiver chez le prestataire ou dans l'OA. **Concerne uniquement les échanges de facturation, et de médico-administratifs.**	L'ensemble des messages échangés est disponible : OUI/NON
	Le logging des erreurs est disponible : OUI/NON
	Les données afférentes à la vérification de la signature faite sur l'ensemble des messages échangés (certificat digital du signataire) sont disponibles : OUI/NON
Description de la procédure d'archivage systématique et complet des données	Description des différentes étapes de l'élaboration du fichier archivé (« comment l'archivage est-il réalisé ?»)
	La périodicité de l'archivage (« quand l'archivage est-il réalisé ?»)
	Le support électronique d'archivage est lisible et pérenne : OUI/NON
ETAPE 2 : CONSERVATION DES ARCHIVES (telles que créées à l'étape 1)	
Description de la procédure décrivant la conservation des archives et leur protection contre toute modification	Lieux de stockage des archives (« où se trouvent les archives ? »)
	Les archives sont dupliquées et conservées dans des endroits physiquement distincts: OUI/NON
	Des moyens de protection entre autres contre la malveillance, le feu, les inondations sont mis en oeuvre : OUI/NON
ETAPE 3 : REPRODUCTION FIDÈLE, DURABLE ET COMPLÈTE DES ARCHIVES	
Description de la procédure garantissant une reproduction fidèle, durable et complète des archives	Le prestataire ou l'OA connaît la démarche à suivre permettant la reproduction fidèle des archives : OUI/NON
	L'accès aux archives peut se faire sur base de différents critères de recherche : OUI/NON

INFORMATIONS RELATIVES A LA SECURITE AUXQUELLES LES ORDINATEURS DU DISPENSATEUR DE SOINS (OU DE SON MANDATAIRE) DOIVENT REPONDRE.	
Firewall	Le firewall interne doit être activé. Ce firewall doit être actualisé en permanence.
	Ne laisser ouvert que quelques ports nécessaires à l'éxécution des tâches professionnelles.
	Opérer une distinction entre les connexions nécessaires au réseau interne et les connexions externes, si applicable.
Anti-virus	Planifier l'éxecution automatique du logiciel anti-malware pour qu'il effectue régulièrement un scan complet du système (tous les fichiers, également les fichiers startup, bios, boot records).
	Utilisez les fonctions real-time présentes dans les programmes anti-malware.
	La mise à jour dui logiciel anti-malware doit être automatique et régulière.
Gestion des patches	Les mises à jour de sécurité doivent d'abord être testées avant leur déployement.
	Après la phase de test, les patches doivent être appliqués automatiquement aussi tôt que possible sur chaque poste de travail dès sa connexion au domaine/réseau.
	Les nouveaux postes de travail ne peuvent être installés sur le réseau que lorsque ces systèmes ont atteint un niveau acceptable en matière de patching.
	En ce qui concerne la fréquence d'installation des mises à jour de sécurité, il convient de trouver un bon équilibre entre les besoins de sécurité et les objectifs opérationnels. Pour les mises à jour qui sont qualifiées d'urgentes par des organismes reconnus il convient de prendre immédiatement les mesures adéquates.
	Une communication régulière doit être prévue entre le service responsable de la gestion des patches des postes de travail et le service réseau. L'objectif est d'évaluer les incidents de sécurité détectés par le service réseau dans le cadre de la gestion des patches et de prendre, le cas échéant, des mesures immédiates.

D'autres informations sont également disponibles auprès de la Banque Carrefour de la Sécurité Sociale:

- « Politique de protection des postes de travail (Information Security Policy) » lors de l'utilisation d'un ordinateur (fixe ou portable)
- « Politique de sécurité PC portable » lors de l'utilisation d'un ordinateur portable