INAMI
Institut National d'Assurance Maladie • Invalidité

Circulaires aux établissements hospitaliers
Circ.Hôp.2003/4

SERVICE DES SOINS DE SANTE

Correspondant : Dr Yves Beterams
Médecin inspecteur
Tél.: 02/739.77.86 **- Fax :** 02/739.77.11
E-mail : hopit@inami.fgov.be
Nos références : 1300/YB/circ.hôp2003/4 **Bruxelles, le**

Echange de données par le biais de Carenet et du protocole de Force probante
Règlement du 17 décembre 2001 (MB 11 avril 2002)

Madame la directrice,
Monsieur le directeur,

Comme suite à la circulaire aux hôpitaux (circulaire 2002/3) du 18 juin 2002, les procédures visées dans l'article 5 du protocole du 19 avril 2001 et dans l'annexe " Procédure Back Office " jointe à ce même protocole, sont rappelées aux établissements de soins qui transmettent les données mentionnées sur les formulaires 721bis - 723 - 725 et 727 par le biais de Carenet.

Il est question ici du protocole, conclu le 19 avril 2001 entre les organisations représentatives des hôpitaux et les organismes assureurs, portant les conditions et les modalités selon lesquelles force probante jusqu'à preuve du contraire peut être accordée aux données qui sont enregistrées ou conservées au moyen d'un procédé électronique, photographique, optique ou de toute autre technique ou communiquées d'une autre manière que sur un support papier, ainsi que les conditions et les modalités selon lesquelles ces données sont reproduites sur papier ou sur tout autre support lisible.

Vous trouverez de plus amples informations à ce sujet dans le dossier "Dispensateurs de soins - Carenet" sur le site de l'Inami : http : //www.inami.fgov.be.

Veuillez agréer, Madame, Monsieur, l'expression de mes sentiments distingués.

Le fonctionnaire dirigeant,

F. PRAET
Directeur général

1.06.01

Protocole, conclu le 19 avril 2001 entre les organisations représentatives des hôpitaux et les organismes assureurs, portant les conditions et les modalités selon lesquelles force probante jusqu'à preuve du contraire peut être accordée aux données qui sont enregistrées ou conservées au moyen d'un procédé électronique, photographique, optique ou de toute autre technique ou communiquées d'une autre manière que sur un support papier, ainsi que les conditions et les modalités selon lesquelles ces données sont reproduites sur papier ou sur tout autre support lisible.

Notification d'hospitalisation et d'engagement de paiement
Demande de prolongation d'hospitalisation
Données en matière d'accord pour la prolongation de la prise en charge de l'hospitalisation
Communication de changement de Service
Notification de fin d'hospitalisation
Données concernant l'identité et l'assurabilité du bénéficiaire

Art. 5. Avant que, en exécution de l'arrêté royal du 27 avril 1999 précité et du présent protocole, force probante puisse être accordée aux données transmises par un hôpital ou un organisme assureur, ces derniers doivent démontrer une seule fois à l'Administrateur général de l'INAMI au moyen d'une liste de contrôle (voir **annexe 3**) qu'ils satisfont aux dispositions figurant dans le présent protocole et ses annexes. Il en sera accusé réception vis-à-vis de l'hôpital concerné ou de l'organisme assureur d'une part, et il en sera donné connaissance dans une circulaire aux organismes assureurs, d'autre part.

Annexe 3 Procédure Back Office

Introduction

Document annexé au protocole CARENET de l'INAMI destiné à définir les conditions nécessaires pour donner et conserver la force probante aux documents transmis via CARENET, énonçant les principes devant être repris pour l'archivage des données pour les différents acteurs CARENET.

Les techniques cryptographiques employées par le GATEWAY CARENET dans les échanges permettent de garantir la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises. Pour que ces éléments de sécurité puissent être utilisés à fin de preuve, il est nécessaire de les conserver de façon sécurisée dans le but de maintenir leur force probante au fil des ans.

Comme les back offices sont par nature différents, il est impossible de décrire précisément une procédure commune. Ce document établi les règles générales que devra respecter l'archivage des données échangées via CARENET afin de pouvoir leur donner force probante et conserver celle-ci. La description complète des procédures est de la responsabilité de chacun des acteurs CARENET.

Procédures applicables en cas de litige

Contestation de la part de l'émetteur:

- Recherche du numéro de BUFFER contenant le message en cause (ou son absence).
- Rechercher ce BUFFER et recalculer la signature faite sur le message CARENET.
- Comparaison de la signature avec l'accusé de réception signé du récepteur

Contestation de la part du récepteur:

- Recherche du numéro de BUFFER contenant le message en cause (ou son absence).
- Rechercher ce BUFFER et recalculer la signature faite sur le message CARENET.
- Contrôle de la signature de l'émetteur

Pièces nécessaires à conserver pour reproduire en cas de litige

L'émetteur d'un MESSAGE CARENET doit conserver:

- L'ensemble du message transmis.
- L'accusé de réception du message transmis.
- Les fichiers logging message et erreur.
- Afin de faciliter les recherches, il serait également nécessaire de conserver le lien entre le message et le numéro de BUFFER créé.

- Les données afférentes à la vérification de la signature de chaque message (certificat digital du signataire, la chaîne de certificat, la liste de révocation des certificats au moment de la vérification)
- L'assurance que toutes ces données sont authentiques et intègres.

Le récepteur d'un message CARENET doit conserver :

- L'ensemble du message reçu.
- L'accusé de réception transmis.
- Les fichiers logging message et erreur.
- Afin de faciliter les recherches, il serait également nécessaire de conserver le lien entre la demande et le numéro de BUFFER reçu.
- Les données afférentes à la vérification de la signature de chaque message (certificat digital du signataire, la chaîne de certificat, la liste de révocation des certificats au moment de la vérification)
- L'assurance que toutes ces données sont authentiques et intègres.

Description fonctionnelle des procédures à mettre en place par les différents acteurs pour assurer l'enregistrement, la conservation et la reproduction des données échangées.

1. Description des données à archiver

- L'ensemble des messages échangés
- La liste des BUFFERS échangés associés à leur HEADER
- Il est obligatoire de conserver le lien entre chaque message et le BUFFER dans lequel il a été transmis. Ce lien doit permettre de déterminer le BUFFER dans lequel un message a été transmis et de reconstituer le BUFFER avec l'ensemble de ses messages
- Le logging des messages du GATEWAY contenant les signatures des messages échangés ainsi que les références des BUFFERS.
- Le logging des erreurs du GATEWAY
- Les données afférentes à la vérification de la signature de chaque message (certificat digital du signataire, la chaîne de certificat, la liste de révocation des certificats au moment de la vérification)
- L'assurance que toutes ces données sont authentiques et intègres.

2. Description de la procédure d'archivage

Journalièrement, l'ensemble des fichiers cités au point 1 sera sauvé en deux exemplaires distincts sur support non volatile. Ces fichiers sauvegardés pourront être concaténées à ceux sauvés antérieurement mais devront, par la suite, pouvoir en être isolées.

3. Description des procédures de conservation des archives

Les archives seront stockées de façon à ce qu'elles ne puissent être ultérieurement modifiées ou que toute modification ultérieure soit détectable. Les archives seront dupliciées et conservées dans des endroits physiquement distincts pour éviter une destruction simultanée en cas d'accident. Ces

archives seront protégées contres toute altération physique (feu, inondation) et, afin d'en préserver le caractère confidentiel, leur accès ne sera possible que par des personnes préalablement désignées.

4. Description de la procédure de recherche dans l'archivage et de publication des archives

L'accès aux données pourra se faire en mentionnant différents critères de recherche dont au moins les critères suivants isolément ou combinés: NISS, date d'envois, date de réception, numéro de message, type de message, numéro de mailbox, institution, fichier. Sauf incidents fortuits et pour autant que l'on se situe durant les heures normales d'ouverture des bureaux, les recherches devront aboutir dans un délai de 4 heures après leur demande. Le résultat de la recherche sera disponible via affichage et une impression de tout ou partie devra être possible.

5. Description des moyens informatiques logiciels et matériel mis en œuvre

Le matériel, logiciels, et supports utilisés seront de large diffusion et devront assurer une pérennité des applications pour une durée au moins équivalente à la durée maximum de rétention. Si la technique utilisée s'avérait ne plus être suivie par le fournisseur, il serait de la responsabilité de l'institution de faire le nécessaire pour récupérer les informations sur un nouveau support.

Remarques

- Chaque étape de la procédure devra garantir la reproduction fidèle durable et complète des informations, prévoir un enregistrement systématique et complet des données.
- Les données archivées seront conservées durant une période de 10 ans, classées et protégées contre toute altération.
- Il sera fait mention des mesures de sécurité prises pour protéger le caractère confidentiel des données.
- Pour chaque étape, un journal de bord doit être tenu dans lequel sera indiqué:
  - l'identité du responsable du traitement
  - l'identité de celui qui a exécuté le traitement
  - le type d'information traitée
  - les date, heure et lieu du traitement
  - les perturbations éventuelles constatées.

- L'ensemble des procédures, du matériel et logiciels utilisés seront décrits en détail dans un dossier régulièrement tenu à jour dont un exemplaire sera remis au conseiller en sécurité de l'institution et un autre sera à la disposition des services de contrôle de l'INAMI.

Rôle du conseiller en sécurité

Le conseiller en sécurité conseillera, de sa propre initiative ou à la demande, le responsable de la gestion journalière de son institution. Il est chargé de rassembler, de tenir à jour et de distribuer la documentation nécessaire. Il est également chargé de veiller à la bonne application des procédures mise en place au sein de l'institution. Il établira annuellement un rapport portant sur le respect effectif des procédures. En tout temps, il devra, s'il constate un quelconque manquement, en faire part immédiatement à la direction de l'institution. Les avis ou rapports seront communiqués de façon écrite et motivée.

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 de l'institution. Elle reprend donc les informations minimums que doit contenir ce dossier pour répondre aux conditions nécessaires afin de donner force probante aux documents électroniques.

GENERALITES	
	Dénomination de l'institution
	Nom du document
	Auteur responsable
	Suivi des versions et mises à jour
	Date d'impression
	Endroit ou il est stocké ou disponible
	Nom du conseiller en sécurité
	Date de dernière délivrance au conseiller en sécurité
	Liste des personnes ayant accès aux données dans les différentes étapes
ETAPE 1: ENREGISTREMENT SYSTEMATIQUE ET COMPLET DES DONNEES	
Nature et objet des informations auxquelles le traitement se rapporte	L'ensemble des messages échangés
	La liste des BUFFERS échangés associés à leur HEADER
	Lien entre chaque message et le BUFFER dans lequel il a été transmis. Ce lien doit permettre de déterminer le BUFFER dans lequel un message a été transmis et de reconstituer le BUFFER avec l'ensemble de ses messages
	Le logging des messages du GATEWAY contenant les signatures des messages échangés ainsi que les références des BUFFERS.
	Le logging des erreurs du GATEWAY
	Les données afférentes à la vérification de la signature de chaque message (certificat digital du signataire, la chaîne de certificat, la liste de révocation des certificats au moment de la vérification)
Description de la procédure d'enregistrement systématique et complet des données	L'environnement
	Les flux
	La périodicité des opérations
	Le contrôle de qualité
	Réaction en cas d'incidents
	Description des moyens et caractéristiques des logiciels mis en œuvre
	Description des moyens et caractéristique du matériel mis en œuvre
	Mesures de protection de la confidentialité des données
Données relatives au traitement devant être conservées	Responsable du journal de bord lieu de consultation de celui-ci ou endroit de stockage
	Identité du responsable du traitement
	Identité de celui qui a exécuté le traitement

	Nature et objet des informations auxquelles se rapporte le traitement
	Date et lieu de l'opération
	Perturbations éventuelles
ETAPE 2: CONSERVATION DES DONNÉES SYSTÉMATIQUEMENT CLASSÉES ET PROTEGEES CONTRE TOUTE ALTÉRATION	
Description de la procédure décrivant la conservation des données systématiquement classées et protégées contre toute altération	Lieux de stockage
	Description des mesures organisationnelles et technique garantissant l'inaltérabilité des données conservées et stockées
	Description des procédure de sauvegarde périodique des back up de données conservées garantissant leur restitution possible.
	Description de la méthode de classement
	Description de moyens de protection entre autre contre la malveillance, le feu, les inondations
	Le contrôle d'accès aux données
	Réaction en cas d'incidents
	Mesures de sécurité prévues afin de protéger le caractère confidentiel des données
Données relatives au traitement devant être conservées	Responsable du journal de bord lieu de consultation de celui-ci ou endroit de stockage
	Identité du responsable du traitement
	Identité de celui qui a exécuté le traitement
	Nature et objet des informations auxquelles se rapporte le traitement
	Date et lieu de l'opération
	Perturbations éventuelles
ETAPE 3: REPRODUCTION FIDÈLE, DURABLE ET COMPLÈTE DES INFORMATIONS	
Description de la procédure garantissant une reproduction fidèle, durable et complète des informations	L'environnement
	Les flux
	Description des moyens d'accès et des critères de recherche des données
	Le contrôle de qualité
	Réaction en cas d'incidents
	Description des moyens et caractéristiques des logiciels mis en œuvre
	Description des moyens et caractéristique du matériel mis en œuvre ainsi que des outputs crées
	Mesures de sécurité prévues afin de protéger le caractère confidentiel des données
Journal de bord	Responsable du journal de bord lieu de consultation de celui-ci ou endroit de stockage
	Identité du responsable du traitement
	Identité de celui qui a exécuté le traitement
	Nature et objet des informations auxquelles se rapporte le traitement
	Date et lieu de l'opération
	Perturbations éventuelles