Protocole, rédigé le 17 mars 2010 par la Commission de conventions praticiens de l'art infirmier - 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 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.

Vu l'article 9bis de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994;
Vu l'arrêté royal du 27 avril 1999, modifié par l'arrêté royal du 26 avril 2007, relatif à la force probante des données enregistrées, traitées, reproduites ou communiquées par les dispensateurs de soins, les organismes assureurs, l'Institut national d'assurance maladie-invalidité et toute autre personne physique et morale en application de la loi coordonnée le 14 juillet 1994 et de ses arrêtés d'application;
Vu la proposition de protocole, établie par la Commission de conventions praticiens de l'art infirmier - organismes assureurs, visée à l'article 17 de l'arrêté royal du 3 juillet 1996 portant exécution de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994;
Vu l'avis du Comité du Service du contrôle administratif de l'Institut national d'assurance maladie-invalidité, émis le 29 mars 2010;
Vu l'avis du Comité du Service d'évaluation et de contrôle médicaux de l'Institut national d'assurance maladie-invalidité, émis le 26 mars 2010;
Vu l'avis du Comité de l'assurance soins de santé de l'Institut national d'assurance maladie-invalidité, émis le 29 mars 2010;
Vu l'approbation, donnée par le Ministre des Affaires sociales le 21 juin 2011,

Article 1er. Pour l'application de ce protocole, on entend par :

1° "INAMI" : l'Institut national d'assurance maladie-invalidité visé à l'article 10 de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994;
2° "nomenclature" : l'annexe à l'arrêté royal du 14 septembre 1984 établissant la nomenclature des prestations de santé en matière d'assurance obligatoire soins de santé et indemnités ;
3° "protocole" : le protocole visé à l'article 2 de l'arrêté royal du 27 avril 1999, modifié par l'arrêté royal du 26 avril 2007, relatif à la force probante des données enregistrées, traitées, reproduites ou communiquées par les dispensateurs de soins, les organismes assureurs, l'Institut national d'assurance maladie-invalidité et toute autre personne physique et morale en application de la loi coordonnée le 14 juillet 1994 et de ses arrêtés d'application;
4° "prestataires de soins »: les prestataires de soins visés à l'article 21quater de l'Arrêté Royal n° 78 relatif à l'exercice des professions de soins de santé – 10.11.1967 – MB 14.11.1967 (L. 10.08.1967), et les groupements de ces prestataires de soins;
5° "organismes assureurs" : les établissements visés à l'article 2, i), de la loi du 14 juillet 1994 susmentionnée.

Art. 2. L'annexe 1 « MyCareNet : Convention entre les organismes assureurs et les prestataires de soins infirmiers à domicile » et l'annexe 2 « MyCareNet : Principes techniques d'échanges et de reproduction des données », ainsi que leurs modifications ultérieures, sont soumises à l'approbation de la Commission de conventions praticiens de l'art infirmier - organismes assureurs, visée à l'article 17 de l'arrêté royal du 3 juillet 1996 portant exécution de la loi du 14 juillet 1994 précitée.

Art. 3. Le présent protocole définit la procédure à suivre pour qu'en exécution de l'arrêté royal du 27 avril 1999 précité, force probante puisse être accordée aux données électroniques communiquées, enregistrées, traitées ou reproduites, énumérées ci-après :

- données en matière de facturation ;
- documents médico-administratifs , notamment les demandes de toilettes et de forfaits, les notifications de soins palliatif et les demandes des prestations techniques spécifiques de soins infirmiers.

La transmission de ces données entre prestataires de soins ou au sein de l'organisme assureur ne relève pas de l'application du présent protocole.

Art. 4. La représentation des prestataires de soins et, le cas échéant, l'identification de leurs mandataires sont définies par l'annexe 1 « MyCareNet : Convention entre les organismes assureurs et les prestataires de soins infirmiers à domicile » du présent protocole.

Art. 5. En exécution de l'article 3 et de l'article 9, 1° et 5° de l'arrêté royal du 27 avril 1999 précité, l'échange de données doit se dérouler conformément aux principes de MyCareNet tels que prévus par l'annexe 2 « MyCareNet : Principes techniques d'échanges et de reproduction des données » du présent protocole.

Art. 6. En exécution de l'article 9, 2°, 3° et 4° de l'arrêté royal du 27 avril 1999 précité, il revient aux systèmes informatiques utilisés par les prestataires de soins et les organismes assureurs de conserver systématiquement et complètement les données échangées, de garantir leur intégrité et leur authenticité et d'en protéger le caractère confidentiel. En outre, les données concernant l'identité du responsable de la transmission ainsi que de celui qui a exécuté cette transmission; une information temporelle complète et les rapports de perturbations éventuelles qui ont été constatés pendant le traitement, doivent être conservées.

La durée de la conservation des données échangées et des rapports de transmission y attenant est identique à celle qui est valable pour le dossier infirmier selon l'article 8 de la nomenclature.

Art. 7. En exécution de l'article 9, 1° de l'arrêté royal du 27 avril 1999 précité, les informations transmises ou reçues doivent pouvoir être fidèlement reproduites sur un support papier lisible, avec identification de la personne qui a transmis les informations originales et l'identification de la personne qui est responsable de l'impression.

Le Service d'évaluation et de contrôle médicaux ou le Service du contrôle administratif doivent pouvoir - à leur demande - avoir accès à ces données par l'impression des données sur support papier comme indiqué ci-dessus; par la consultation des données sur un écran d'ordinateur, un terminal ou une station de travail ou par la mise à disposition des données sur un support électronique.

Art. 8. La surveillance du bon respect des dispositions du présent protocole et de ses annexes est assurée respectivement par le Service d'évaluation et de contrôle médicaux et le Service du contrôle administratif, chacun au niveau de ses compétences.

Sans préjudice de leurs propres compétences spécifiques, les Services de contrôle doivent communiquer les éventuelles lacunes ou irrégularités à la Commission de conventions praticiens de l'art infirmier - organismes assureurs, visée à l'article 17 de l'arrêté royal du 3 juillet 1996 portant exécution de la loi du 14 juillet 1994 précitée.

Annexe 1

MyCareNet – Convention entre les organismes assureurs et les prestataires de soins infirmiers à domicile.

Objectif

L'objectif de cette convention est de fixer, complémentairement à la réglementation, les règles de travail pratiques et impératives pour l'échange électronique de données via le réseau MyCareNet entre prestataires de soins infirmiers à domicile et les organismes assureurs.

Définitions

- **Organisme assureur**: les organismes visés à l'article 2,i) de la loi du 14 juillet 1994.
- **Prestataire de soins**: les prestataires de soins visés à l'article 21quater de l'Arrêté Royal n° 78 relatif à l'exercice des professions de soins de santé – 10.11.1967 – MB 14.11.1967 (L. 10.08.1967), et les groupements de ces prestataires de soins.
- **Réseau**: le réseau MyCareNet
- **Service**: type de transmission de données (consultations d'assurabilité, facturation, volet médico-administratif) auquel le prestataire de santé souhaite adhérer.
- **Mandat**: l'acte juridique entre deux entités juridiques dont l'une entité (le mandant) autorise l'autre entité (mandataire) pendant une période déterminée, à avoir l'accès au réseau MyCareNet pour un service particulier, et ce au nom du mandant.
- **Mandant**: entité identifiée qui donne mandat.
- **Mandataire**: entité identifiée qui reçoit mandat pour avoir accès au réseau MyCareNet pour un service particulier, et ce au nom du mandant.

Droits et obligations des parties

- **Droits et obligations des organismes assureurs**
  - Disponibilité des services :
    - Au niveau technique (disponibilité du réseau MyCareNet) :
      - En principe, les prestataires de soins peuvent introduire leurs demandes 24 heures sur 24 heures. En dehors des heures de bureau, les organismes assureurs y réagiront sur base du meilleur effort (best-effort).
    - Au niveau du Helpdesk de MyCareNet :
      - le helpdesk sera disponible pendant les heures de bureau de 8H à 18H, et ce uniquement pendant les jours ouvrables. Un document séparé mentionnera où le prestataire de soins pourra s'adresser et avec quelles questions.
    - Au niveau des Helpdesk des organismes assureurs :
      - le helpdesk sera disponible pendant les heures de bureau de 9H à 12H et de 13H30 à 16H et ce uniquement pendant les jours ouvrables. Un document séparé mentionnera où le prestataire de soins pourra s'adresser et avec quelles questions.
    - La coordination entre les services Helpdesk de MyCareNet et des OAs sera assurée.

- **Droits et obligations des prestataires** :
    - Les prestataires de soins sont responsables pour l'exactitude et la mise à jour en temps utile de leurs données dans les sources authentiques (Par exemple : en tant que responsable de groupement vis-à-vis de l'INAMI, en tant que responsable d'entreprise vis-à-vis de la banque carrefour des entreprises, …).
    - Les éventuelles futures adaptations à cette convention seront approuvées par la Commission de Convention praticiens de l'art infirmier. La version la plus récente de cette convention peut à tout moment être obtenue auprès du Collège Intermutualiste National.
    - Un prestataire de soins a accès au réseau pour autant qu'e-health reconnaisse et authentifie les identifiants et qualités que lui présente le prestataire de soins.
    - L'utilisation de ce réseau pour un service (consultation assurabilité, facturation, volet médico-administratif) sous-entend l'acceptation automatique des conditions relatives à ce service comme stipulées dans l'annexe correspondante.
    - Le helpdesk première ligne du prestataire de soins est toujours le fournisseur du logiciel au moyen duquel le prestataire consulte My Carenet (donc en cas de problème avec MyCareNet, le prestataire de soins contactera son fournisseur de logiciel).
    - Le prestataire de soins s'engage à consulter régulièrement les messages (réponse) des organismes assureurs via la mailbox prévue afin d'être toujours au courant des communications des organismes assureurs (accord, refus, adaptation forfait par le médecin conseil, …).
    - Les données mises à disposition du prestataire via MyCareNet (download) le sont pour une période de trois mois maximum.
    - En cas d'abus ou d'infraction à la présente convention :
        - Dès qu'un organisme assureur constate des abus ou des infractions à la présente convention, il enverra au prestataire de soins un avertissement à ce sujet par lettre recommandée.
        - En cas de répétition des faits endéans les 365 jours, la Commission de convention praticiens de l'art infirmier, les services de contrôles administratifs et médicaux de l'INAMI en seront informés, et prendront, en fonction de leurs compétences et responsabilités respectives, les actions nécessaires vis-à-vis du prestataire de soins.
        - Le CIN fera part de tout cas d'abus le concernant au Comité sectoriel de la sécurité sociale et de la santé, qui veille au respect de la protection de la vie privée des assurés sociaux dans le service concerné.
    - Au cas où l'utilisation du réseau par le prestataire de soins mettrait en danger la disponibilité ou la sécurité du système informatique, l'accès pourrait temporairement lui en être refusé, le temps que le problème soit résolu (Il s'agit ici de '*problèmes techniques'*).

Représentation

Si le prestataire de soins est une personne physique, il/elle agira en son propre nom.
Si le prestataire de soins est une personne juridique, il/elle sera représenté(e) par une personne désignée à cet effet dans les statuts de cette personne juridique.
Si le prestataire de soins est une association de fait, le représentant communiqué à l'INAMI par l'association, agit également comme représentant au niveau de la présente convention.
Le prestataire de soins reste toujours civilement responsable pour les actes des personnes à qui il/elle confie une part de son activité.
Les organismes assureurs ne tiendront compte que des documents signés par le représentant légal d'un prestataire de soins ou par une personne désignée mandatée à cet effet. Cela ne vaut pas pour les documents électroniques qui sont soumis à leurs propres règles.
Conformément à l'art. 9 bis W 14.7.94, il peut être accordé force probante aux données échangées via le réseau (Modalités définies dans un 'protocole force probante').

Mandats

Un prestataire de soins a le droit de donner un mandat à un mandataire.
Un mandat doit être confirmé par écrit selon le modèle en vigueur sur la plateforme e-health (https://www.ehealth.fgov.be/fr/page_menu_a_m/website/home/portal/access/mandates.html).
Le mandataire doit porter ce mandat à la connaissance du Collège Intermutualiste National.
La période pour laquelle le mandat est donné, doit être reprise explicitement dans ce mandat. Le mandat doit parvenir au CIN au moins 5 jours ouvrables avant la date de prise d'effet du mandat.
Le mandant reste responsable du contenu des messages et plus spécifiquement du contenu de la facturation et de l'effectivité des prestations fournies.
Les prestataires de soins dont les prestations sont attestées via un numéro de groupe (tel qu'on l'entend sur le site de l'INAMI : **http://www.inami.fgov.be/**) ne doivent pas donner de mandat MyCareNet.

Pour être valables, les mandats doivent répondre aux conditions énumérées limitativement ci-après :

- Le mandat doit mentionner explicitement l'objet du mandat. Un mandat vaut uniquement pour maximum 1 service (consultation assurabilité, facturation ou volet médico-administratif).
- Un mandat n'aura pas trait à la façon de payer. A cet effet, un accord spécifique doit être signé entre le prestataire de soins et l'organisme assureur.
- La date de la signature doit être reprise explicitement de sorte que l'organisme assureur puisse vérifier quand ce mandat produira ses effets.
- Il ne peut pas y avoir de périodes chevauchantes entre 2 mandats pour un même service. Le cas échéant, un nouveau mandat pour un service clôture automatiquement le mandat précédent.
- En cas de décès, de faillite ou de liquidation du mandant ou du mandataire, tout mandat est immédiatement terminé. Un nouveau mandat peut éventuellement être donné par ou avec le liquidateur ou le curateur.

Evaluation

Il sera fait une évaluation permanente de cette convention.

Annexe ‘Service Facturation’

Objectif

L’objectif de cette annexe est de fixer les règles de travail pratiques et impératives pour l’échange des données électroniques dans le service « facturation ».

Définitions

La **facturation** est la transmission des factures et la réponse à celle-ci d’un point de vue administratif entre les prestataires de soins et les organismes assureurs par voie électronique et dans le régime du tiers payant.

Droits et obligations des parties

- Droits et obligations des organismes assureurs

  - Les organismes assureurs s’engagent à traiter les factures dans les délais comme stipulé dans les conventions entre les organismes assureurs et les prestataires de soins concernés.
  - Les factures ne seront considérées comme reçues que si l’accusé de réception de l’organisme assureur a été renvoyé via le réseau.
  - Les organismes assureurs sont tenus à un engagement de paiement conforme aux conditions de l’art. 159 AR 3.7.96, revu par l’AR du 5 juin 2008.

- Droits et obligations des prestataires de soins

  - Le prestataire de soins s’engage à ne plus transférer des supports magnétiques aux organismes assureurs à partir du moment où il envoie les fichiers de facturation via MyCareNet.
  - Le prestataire de soins traitera les données avec stricte confidentialité.

Annexe ‘Service Assurabilité’

Objectif

L’objectif de cette annexe est de fixer les règles de travail pratiques et impératives pour l’échange des données électroniques dans le service « assurabilité »

Définitions

Assurabilité: la confirmation de données pour vérifier les droits aux remboursements par l’assurance maladie-invalidité, ainsi que des données pour l’application du tarif de remboursement, statut et de la période pour laquelle ces données sont valables. Cette consultation sera faite soit ‘on-line’ pour un patient, soit ‘en différé’ pour un ou plusieurs patients à la fois.

Droits et obligations des parties

- **Droits et obligations des organismes assureurs**
  - Les organismes assureurs s’engagent à toujours fournir les informations disponibles les plus actuelles.
  - Les réponses au niveau du service assurabilité sont données endéans le premier jour ouvrable qui suit la demande et ce pour 95% des demandes. Ce pourcentage est calculé sur l’ensemble des demandes (assurabilité ‘on-line + assurabilité ‘en différé’).
  - Les organismes assureurs sont obligés de mettre à disposition les données dont les prestataires de soins ont besoin afin d’être en mesure de pouvoir correctement facturer leurs prestations.

- **Droit et obligations des prestataires de soins**:
  - Le prestataire de soins s’engage à ne solliciter et traiter des données que pour des patients qu’il traite effectivement et ce dans le but exclusif de la facturation des traitements médicaux.
  - Le prestataire de soins s’engage à procéder effectivement à la facturation pour minimum 99% des patients pour qui il/elle a sollicité les données relatives à l’assurabilité.
  - Le prestataire de soins traitera les données avec stricte confidentialité et ne les transmettra pas à d’autres prestataires de soins ni à des tiers.
  - La règle de base est la suivante : Pour un même traitement d’un patient, le prestataire de soins ne pourra solliciter qu’une seule fois de manière informative les données relatives à l’assurabilité au début du traitement et ensuite maximum une fois par mois en vue de la facturation. Des exceptions seront acceptées pour des situations particulières (patient non en règle à recontrôler, etc…).

Annexe 'Volet Medico-administratif'

Objectif

L'objectif de cette annexe est de fixer les règles de travail pratiques et impératives pour l'échange des données électroniques pour le volet médico-administratif.

Définitions

Volet médico-administratif : Il s'agit de l'envoi électronique des notifications et des demandes du prestataire de soins à l'organisme assureur pour les soins infirmiers à prester auprès du patient et les réponses électroniques de l'organisme assureur au prestataire. Les directives de l'article 8 de la nomenclature valent comme base légale pour ces échanges électroniques. Le volet médico-administratif est composé de 3 domaines ; les demandes de toilettes et de forfaits A, B et C se font via les messages 410xxx ; les notifications de soins palliatifs se font via les messages 420xxx ; les notifications des prestations de soins techniques spécifiques se font via les messages 430xxx.

Droits et obligations des parties

- **Droits et obligations des organismes assureurs**

    - Les organismes assureurs s'engagent à toujours fournir les informations disponibles les plus actuelles (Les informations échangées sont décrites dans les descriptions des messages MyCareNet).
    - Les organismes assureurs s'engagent à mettre à disposition les réponses relatives au volet médico-administratif dans un délai raisonnable.
    - Les notifications et les demandes ne seront considérées comme arrivées aux OA que lorsque MyCareNet aura mis à la disposition du prestataire un '*accusé d'envoi*' avec la date et l'heure à laquelle MyCareNet a reçu le message correspondant. En cas de litige, c'est au prestataire de prouver qu'il est en possession de l'accusé d'envoi. L'accusé d'envoi n'est pas un accord de l'OA pour l'intervention financière de l'AMI pour les soins demandés.
    - Les organismes assureurs s'engagent à mettre une réponse à la disposition du prestataire demandeur lors de chaque notification ou demande. Cette réponse peut être un rejet (si message non traitable - erreurs formats, etc…), un accusé de réception (preuve que l'OA a bien reçu et enregistré le message - exemple : accusé de réception d'une notification prestation technique spécifique), une acceptation (demande accordée par le médecin conseil) ou un refus (demande refusée par le médecin conseil). C'est cette réponse qui définit ou non l'intervention financière de l'AMI pour les soins demandés.
    - L'adaptation d'un forfait suite à une décision du médecin-conseil est considérée comme d'application le jour où l'OA en informe le prestataire.

- **Droit et obligations des prestataires de soins**:
    - Le prestataire de soins s'engage à contrôler en premier lieu l'affiliation mutualiste de son patient avant l'envoi électronique de la notification ou de la demande. Ainsi le prestataire de soins peut toujours envoyer la notification ou la demande vers l'organisme assureur correct.
    - Le prestataire de soins traitera les données avec stricte confidentialité et ne les transmettra à d'autres prestataires de soins que pour garantir la continuité des soins.
    - Le prestataire se porte garant pour la conservation dans le dossier du patient de toutes les attestations, prescriptions, plans de traitement, … décrits dans la nomenclature pour laquelle l'emploi de MyCarenet leurs permet de ne plus devoir les transmettre à l'organisme assureur. Ces documents doivent rester à la disposition du médecin-conseil lors d'une visite ou sur simple demande. Ces documents doivent également rester à la disposition du Service d'évaluation et de contrôle médicaux pour ce qui concerne ses compétences.

Annexe 2 : Solution MyCareNet : Principes techniques d'échange et de reproduction des données

Introduction

MyCareNet est une solution élaborée par les organismes assureurs pour l'échange sécurisé d'informations structurées avec les prestataires de soins au travers du réseau Internet.

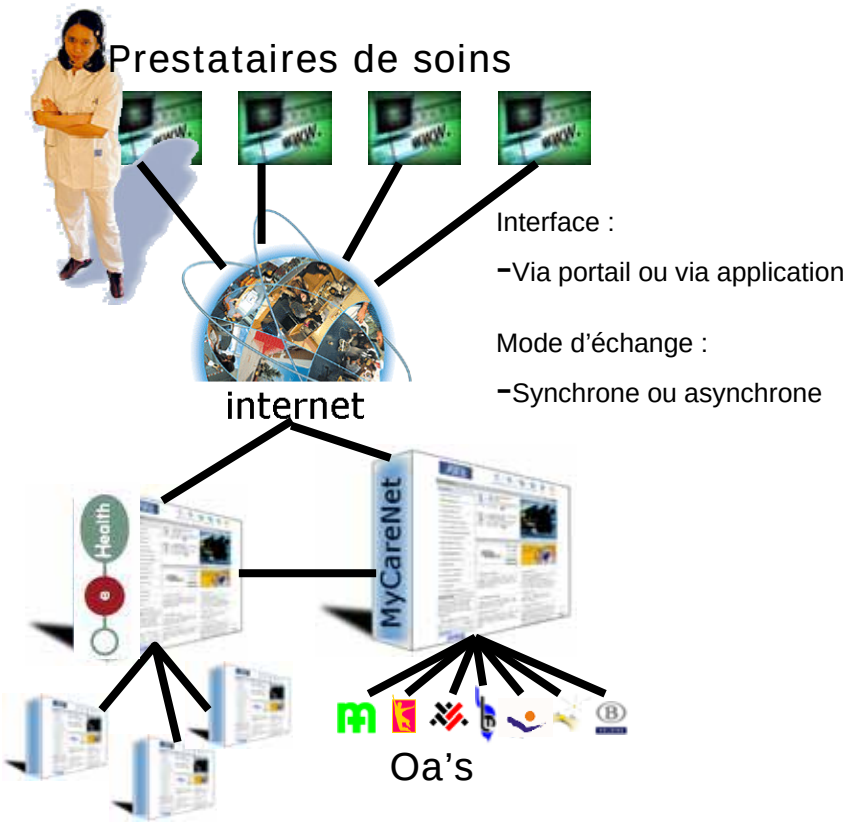
MyCareNet est une évolution de la solution CareNet opérationnelle depuis plusieurs années pour les échanges avec le secteur hospitalier.

D'un point de vue informatique, la solution MyCareNet comporte :

- Des composants d'infrastructure et notamment une plateforme informatique qui coordonne les échanges. Cette plateforme d'échange est gérée par le Collège Intermutualiste National (CIN) au nom des organismes assureurs (OA).
- Des traitements informatiques de l'information propre à chaque application particulière (ex : assurabilité) tant chez le prestataire, que dans chaque OA ainsi que sur la plateforme MyCareNet.
- Des services informatiques externes fournis principalement par la plateforme eHealth

La solution MyCareNet intègre également :

- Des services et procédures de gouvernance : helpdesk, service management, maintenance évolutive et corrective, gestion des adhésions et des tests, capacity management, etc.
- Des aspects réglementaires qui dictent son organisation et son usage en fonction de la législation et notamment des directives des organismes de tutelle ainsi que des exigences de respect de la vie privée.



Le schéma ci-dessus donne un aperçu général sur l'architecture du réseau mise en œuvre et sur ses principaux composants :

- le réseau de télécommunication : Internet tenant compte de sa généralisation, de son faible coût d'utilisation, des techniques existantes permettant d'enrober la communication et les informations transmises de toute la sécurité nécessaire ;

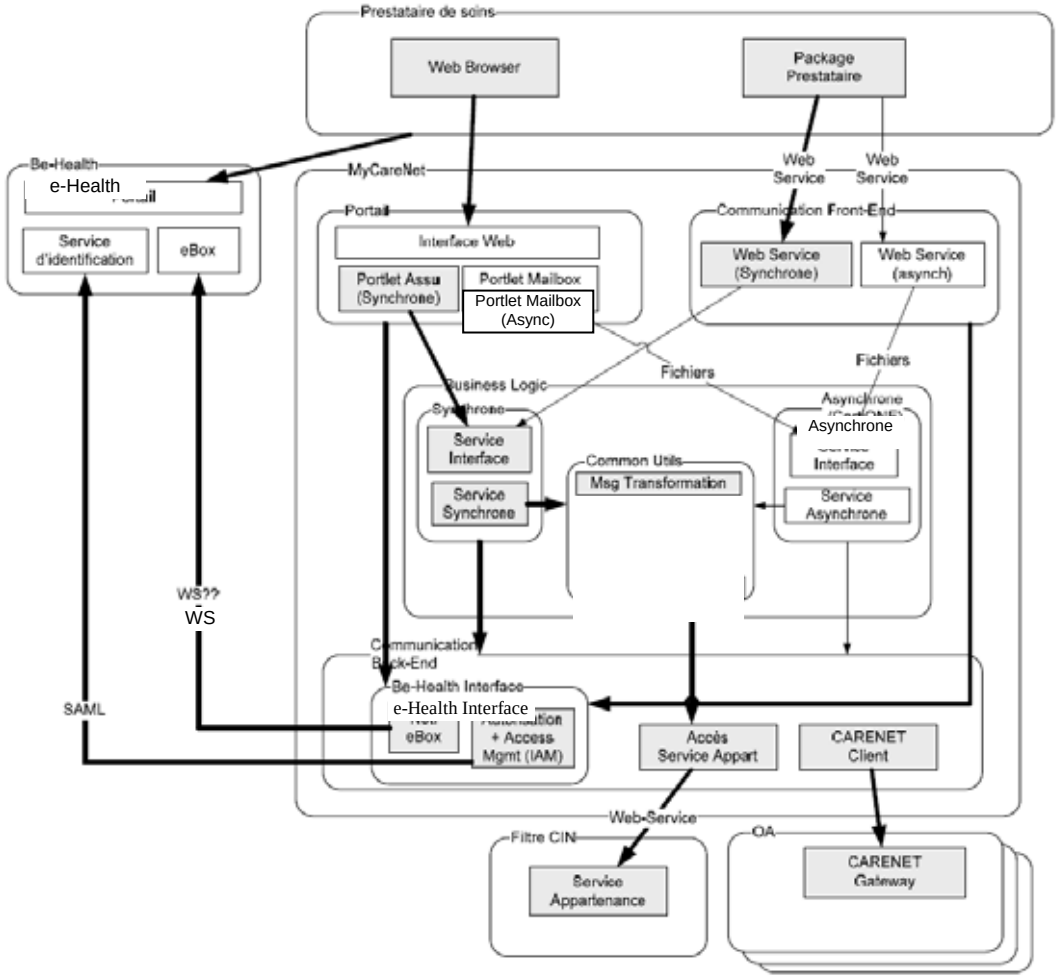
- le poste de travail du prestataire : c'est le prestataire qui, au départ de son poste de travail, via portail ou via son application, initie tout type de communication avec les organismes assureurs ;

- le portail e-Health : il offre la possibilité de se connecter aux différents portails du secteur soins de santé

- le portail MyCareNet : créé et géré par le CIN, ce portail, outre des fonctions utilitaires complexes, permet de mettre en connexion le prestataire et l'organisme assureur en fonction de l'appartenance mutualiste du patient. Le portail "MyCareNet", sur la base du profil du prestataire, propose un panel de fonctionnalités que le prestataire choisit en fonction des besoins du moment.

Description des flux (y compris méthode d'encryptage)

Architecture logique



En standard, MyCareNet dispose de deux interfaces permettant à un prestataire de soins de faire appel à ses applications.

- Système à système
  Dans ce cas, l'application de l'utilisateur doit être capable de faire appel à des « web services », une technologie qui permet de communiquer selon des standards, quel que soit le langage et les outils de développement des applications cliente et serveur.
  Cette communication permet une intégration maximale des services et des données échangées. L'application de l'utilisateur doit aussi être capable de visualiser les différents messages échangés.

- Le portail
  Dans ce cas, l'utilisateur se connecte directement au portail (site web) de MyCareNet qui lui présente ses services sous forme de pages HTML.
  Selon les services, MyCareNet travaille avec des formulaires d'introduction des requêtes et de visualisation des réponses et/ou via des fonctions de chargement/déchargement de fichiers.

  Bien que l'intégration soit moindre, cette solution permet à des utilisateurs de faire appel aux principaux services avec un minimum de développement applicatif. Cette solution s'avère également utile si son application n'est pas compatible avec la technologie des webservices.

Quant à ses modes de fonctionnement, MyCareNet permet des échanges :

- 'Online' aussi appelés 'synchrones' :
  Dans ce cas, MyCareNet donne une réponse à une question unique dans un délai raisonnable de quelques secondes qui est compatible avec l'organisation pratique du travail pour le prestataire.

- 'Batch' aussi appelés 'asynchrones' ou « en différé » :
  Une ou plusieurs demandes sont envoyées en un lot vers MyCareNet qui en assure le routage vers leur(s) destination(s).
  Les réponses aux requêtes sont préparées dans un délai convenu de l'ordre de quelques heures ou quelques jours (selon les services).
  Il appartient alors à l'utilisateur d'interroger sa « boîte aux lettres » (mailbox) pour suivre le processus et ensuite pour rapatrier les lots de réponses.
  Ce mode s'applique principalement aux processus nécessitant une intervention humaine (par exemple l'accord d'un médecin conseil)
  Les solutions batch permettent aussi aux organismes assureurs de transmettre, dans certains cas, des informations de leur propre initiative (sans question préalable).

La plateforme MyCareNet contient un bloc "business logic" qui comprend 3 modules:

- *Module synchrone*

Traite les questions (inbound) et les réponses (outbound) sur lesquelles le demandeur attend une réponse immédiate (synchrone).

- *Module asynchrone*

Traite les demandes asynchrone (batch). Le statut interne des demandes pendant le traitement est disponible via le suivi du statut des messages.

- *Module "utilitaires communs"*

Contient des fonctions pour le traitement des messages qui peuvent être utilisées tant par le module synchrone que le module asynchrone.

La plateforme MyCareNet utilise les services de base d'eHealth suivants :

- site portail
- gestion intégrée des utilisateurs et des accès (y compris les mandats)
- boîte aux lettres électronique sécurisée (eBox)

Ces services sont documentés sur **www.ehealth.fgov.be**.

La plateforme MyCareNet utilise également le service d'appartenance mutualiste du Filtre CIN.

Pour communiquer avec les OAs, la plateforme MyCareNet échange des messages au travers du réseau Carenet en utilisant un gateway Client. Côté OA se trouve un gateway Server. Ces gateways se chargent de la signature et de l'encryption des informations transmises sur ce réseau en utilisant des certificats spécifiques. Le document « carenet user's guide « administration and programming » » décrit le fonctionnement des gateways et est disponible sur **www.mycarenet.be**.

Description des flux

Les différents flux transitant au travers de la plateforme d'échange MyCareNet sont décrits dans le document « MyCareNet - Care Provider Implementation Guide », disponible, en anglais, auprès du collège intermutualiste national (CIN).

Dans la description des flux de facturation et des flux médico-administratif, il est à souligner que l'information signée telle que reçue du prestataire est aussi transmise à l'OA à des fins de contrôle d'intégrité et vice versa.

Contenu et format des messages (dont accusés de réception et messages d'erreurs)

Le contenu et format des messages, présents dans les flux transitant au travers de plateforme d'échange MyCareNet, et validés par la commission des messages électroniques et le Comité de l'assurance soins de santé, sont publiés sur le site **www.mycarenet.be**.

Les fichiers transmis dans les messages de facturation respectent le layout prescrit dans les instructions de facturation sur support magnétique ou électronique de l'INAMI et est consultable sur le site **www.inami.fgov.be**.

Méthode d'encryptage

Entre le prestataire et MyCareNet, une encryption basée sur SSL/TLS est réalisée, conformément aux avis n° 07/070 du 04/12/07 et n° 07/003 du 09/01/07, quand requis, du Comité sectoriel de la Sécurité sociale et de la Santé Section « Sécurité Sociale ».
Entre MyCareNet et les OAs, l'encryption réalisée dans CareNet avec chiffrement triple DES avec clef de 128 bits est décrite sur le site **www.mycarenet.be**.

Identification, authentification et autorisation des prestataires de soins

Pour rappel,

L'**authentification** est la procédure qui consiste, pour un **système informatique**, à vérifier l'**identité** d'une entité (**personne**, **ordinateur**...), afin d'autoriser l'accès de cette entité à des **ressources** (**systèmes**, **réseaux**, **applications**...). L'authentification permet donc de valider l'authenticité de l'entité en question.

L'**identification** permet de *connaître* l'identité d'une entité alors que l'**authentification** permet de *vérifier* cette identité.

Dans le cas des interactions système à système

Avant de pouvoir faire appel aux webservices fonctionnels de MyCareNet ou de eHealth, il faut d'abord avoir ouvert une « session MyCareNet ».

En pratique, l'utilisateur va tout d'abord s'identifier et s'authentifier en temps que personne grâce à la lecture de son numéro d'identification au registre national sur sa carte d'identité électronique.[1]

Grâce au certificat d'authentification (protégé par le pincode), il va signer une requête d'ouverture de session qu'il va adresser sous forme d'un webservice particulier à MyCareNet.

MyCareNet va authentifier le numéro d'identification au registre national de l'utilisateur, notamment en effectuant un contrôle de validité du certificat.

MyCareNet va répondre à la requête d'ouverture de session qui sera matérialisée par une paire de clé valable pour la durée de la session ou technique équivalente.[2]

Chaque requête via webservice sera signée au moyen de la clé privée de session, ce qui en garantit l'authenticité et l'intégrité.

La session correspond donc à la période pendant laquelle l'identification et l'authentification de l'utilisateur en tant que personne restent valides pour MyCareNet.

La session peut être établie pour une durée fixée par la requête mais qui ne peut dépasser un maximum. Ce maximum est fixé actuellement à 12 heures (également valeur par défaut) et il est révisable sur demande dûment motivée.

Un webservice particulier permet à un utilisateur de clôturer sa session de manière prématurée, notamment lorsqu'il quitte définitivement son poste de travail.

Une session ne peut être prolongée mais une nouvelle session peut être ouverte ce qui implique en pratique une relecture de la carte d'identité.

En ce qui concerne le contrôle des autorisations, l'utilisateur va, dans un premier temps, identifier le prestataire (numéro inami) pour lequel il souhaite travailler ainsi que le rôle qu'il veut assumer (par exemple en cas de mandat).
Ceci sera codé dans une structure dénommée « sender ».

L'utilisateur va également préciser le type de requête qu'il veut adresser (une interrogation du droit du patient, par exemple).

Chaque appel à un webservice fonctionnel comportera ces deux éléments.

[1] D'autres moyens sont à l'étude , notamment d'autres certificats Fedict
[2] La technique d'ouverture de session basée actuellement sur le protocole XKMS est décrite en détail dans le document « MyCarenet – Care Provider implementation Guide ».

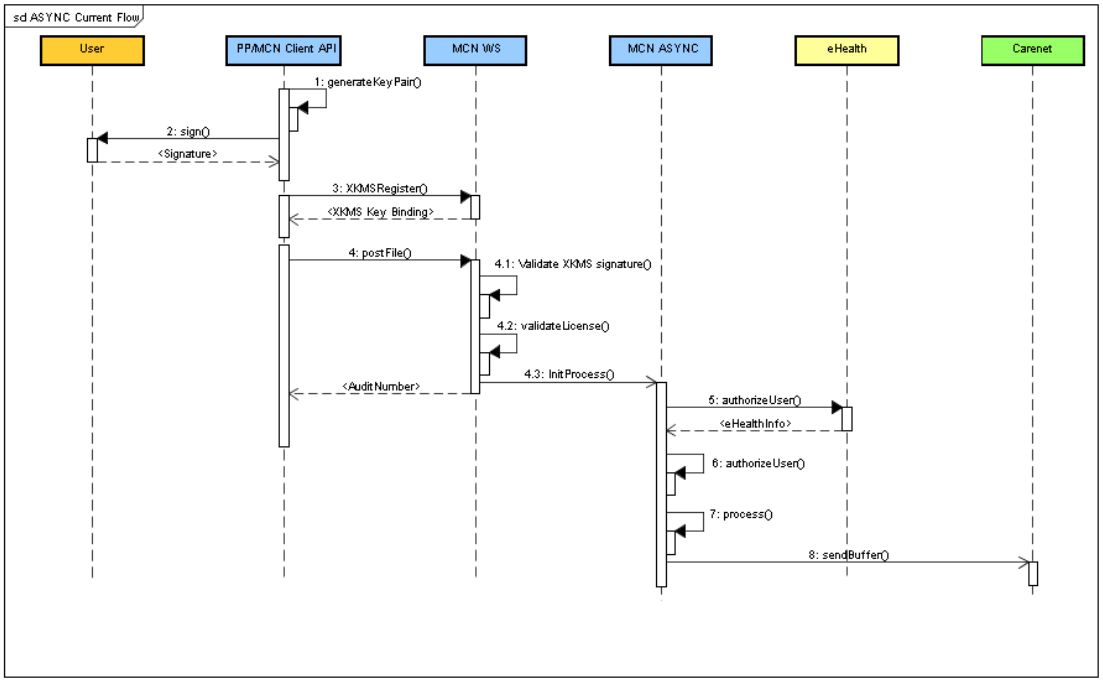
A l'analyse de la requête, MyCareNet transmettra à eHealth l'information d'identification ainsi que la traduction du rôle que l'utilisateur veut assumer.
Sur base notamment de la consultation de sources authentiques, eHealth répondra par une autorisation primaire ou un refus.

En cas d'autorisation, eHealth fournit également certains attributs par exemple sur la durée de validité des mandats. Sur base de ces informations et de règles d'autorisation spécifique au service demandé, MyCareNet va ensuite procéder à un second contrôle d'autorisation.

L'information d'autorisation (Numéro identification national-prestataire-rôle-service demandé) est placée dans une cache de l'application MyCareNet. Des règles de sécurité gèrent la durée de validité de l'information dans cette cache dont l'objectif est de ne pas devoir systématiquement répéter le processus d'autorisation.

Lors des requêtes suivantes, MyCareNet détecte tout changement éventuel à un des paramètres entrant en ligne de compte pour l'autorisation. Dans ce cas ou si l'information de la cache est expirée, MyCareNet reprend le processus complet d'autorisation.

Le schéma ci-dessous illustre un exemple des différentes interactions dans le cas de l'échange asynchrone :

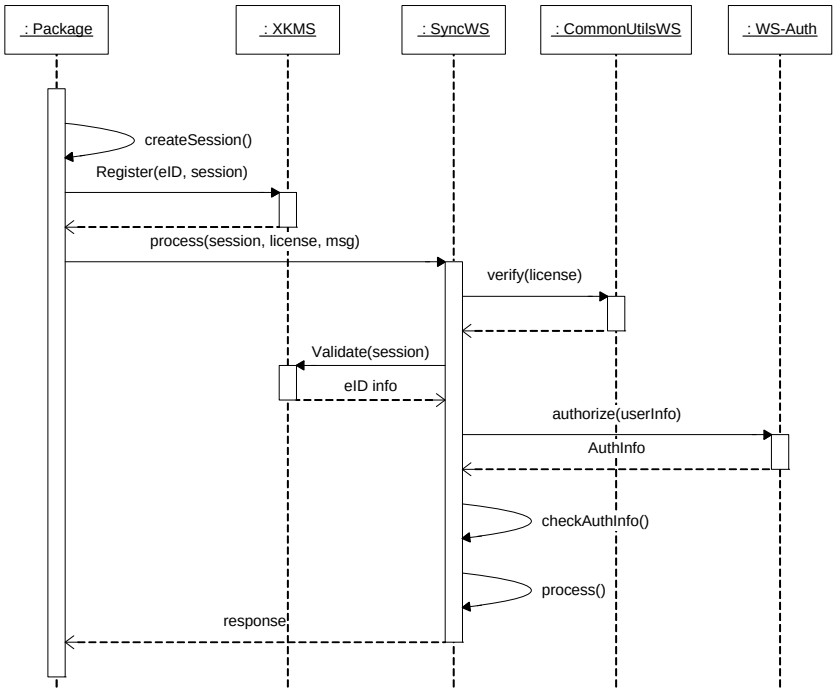


Currently the SDK communicates with the MCN ASYNC platform via an XKMS session:

1. The Client SDK generates a new public/private key pair (if no valid pair is already available from previous interactions).
2. The public session key is signed with the private session key (through eID or Certificate) to provide Proof of Possession. A self-signed certificate is generated. The message towards the MCN platform is also signed with the private key of the eID or client certificate to do Authentication Binding.
3. An XKMS session is instantiated and the generated public key is registered with the MCN platform. MCN validates both the proof of possession and authentication binding against the associated certificates. The generated key pair is used for all further communication (for a defined validity period) between the SDK and MCN platform during the session.
4. New WS requests are signed and validated using the generated keys. The PP license username and password are validated. In case of postFile calls, MCN instantiates the relevant ASYNC process and immediately returns an audit number.

5. At the beginning of the process, MCN contacts the eHealth authorization service to validate all relevant information (INSS, NIHII, groups, mandates,…).
6. Based on the eHealth response, the user authorization takes place. Subsequently, black-white list authorization is also performed.
7. After successful authorization, the process continues.
8. Finally, if the processing is successful, the relevant files are posted towards Carenet via the Carenet Gateway Client.

Le schéma ci-dessous illustre un exemple des différentes interactions dans le cas de l'échange synchrone :



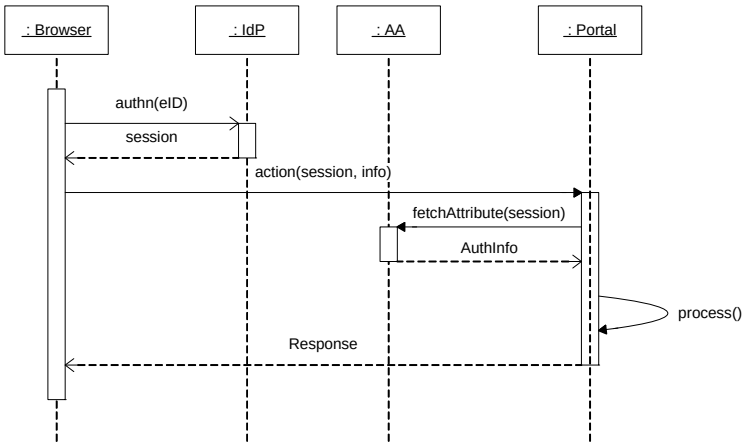
1. First of all the package must generate a session, basically a self signed X509 Certificate.
2. He can then register this session with MyCareNet via XKMS. For this he needs the eID of the person. From this moment MyCareNet has a link between the session and a physical person.
3. The package sends a message to be processed to MyCareNet. For this he must also provide the session he created and registered before and a license (username/password) he received when subscribing to MyCareNet.
4. Sync WS will verify this license
5. It will also validate the session. It does that with XKMS and receives the info of the eID that is used to register the session. At this moment Sync WS knows the physical person
6. Sync WS uses the info about the physical person and the caller info in the message to check with the WS-Auth of eHealth if it is an actual care provider. With this it receives extra information.
7. This extra information is checked by MyCareNet to see if the user has the right to use MyCareNet. This check consists of several sub-checks (e.g. B/W Lists)
8. The message is processed, since this does not change from the current processing, no detail is included in this document.
9. The response is returned to the package.

Dans le cas de l'utilisation du portail

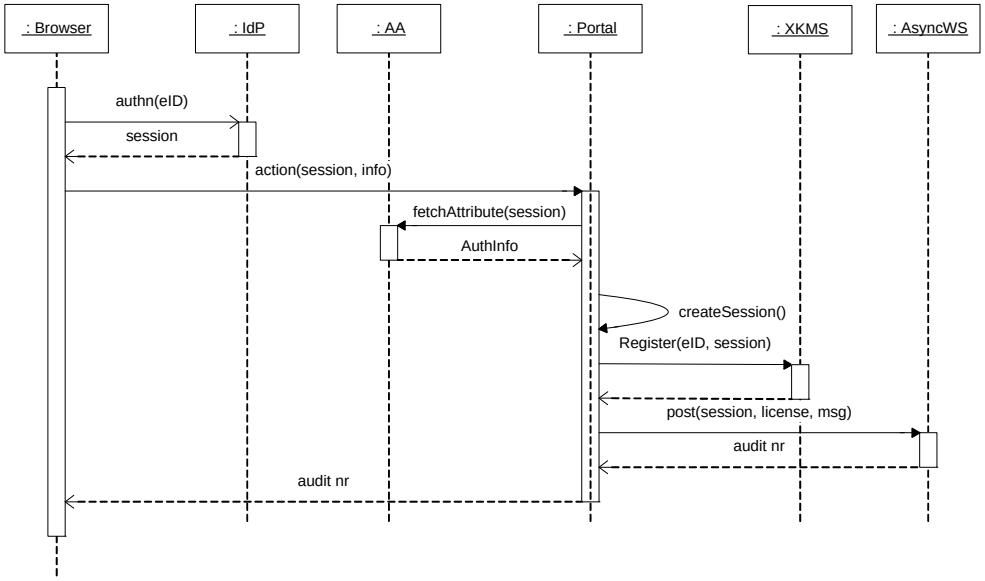
L'utilisation du portail se base sur des principes similaires à ceux des interactions système à système mais elle fait appel à d'autres protocoles (Shibboleth).

Shibboleth est un middleware basé sur SAML, qui implémente un mécanisme d'authentification et d'autorisation inter-domaine (Web Single SignOn) : l'identity provider (IdP) fournit l'information relative aux utilisateurs pendant que le service provider (SP) utilise cette information pour accorder ou non l'accès à certaines ressources. Son utilisation sur la plateforme MyCareNet permet de déléguer l'authentification et la gestion des utilisateurs à eHealth. Sur base de leurs attributs, MyCareNet accorde ensuite à ces utilisateurs l'accès à tel ou tel service.

Le schéma ci-dessous illustre un exemple des différentes interactions dans le cas d'utilisation du portail



1. The user authenticates with its eID (or token) on the Shibboleth IdP of eHealth. Although the user does not notice it, but he get a (SAML) token that can be used to authenticate with MyCareNet (and other SPs)
2. The browser of the user will transfer this token to the MyCareNet portal.
3. Behind the scene, the portal will get all the info of the Shibboleth AA. The returned info is in the same format as WS-Auth of eHealth.
   The portal will send a new token to the browser, this time a cookie. Now the browser knows to reuse this cookie for each consequent call.
4. The portal will accept a new request, check the cookie and execute the requested action
5. The portal sends the response to the browser to be displayed for the user.



1. The basic authentication is exactly the same as before
2. When the portal detects it needs to forward the request, it creates a new session. Currently it is an self signed certificate
3. It registers the session with XKMS, for this it does not use the eID of the user but creates a dummy eID using a special CA certificate. XKMS knows it is a dummy eID, but trusts it anyway because it knows only the portal has the private key of that specific CA certificate.
   The reason to use a dummy eID and not use the real eID of the user is because the user is already authenticated. He will not accept to have to re-authenticated for a, for him, arbitrary reason.
4. Once the portal has registered his session, it can use this to forward the message to the Async WS. Off course the portal uses a different session per physical user.
5. The portal receives the audit number and return it to the browser.

Signature et datation des messages

Les fichiers de facturation et les documents médico-administratifs échangés au sein de l'enveloppe MyCareNet (appelée CPD pour Care Provider Document) doivent être signés électroniquement à des fins d'intégrité, aussi bien dans le mode de fonctionnement du système à système que celui du portail.

Cette signature est à appliquer globalement sur l'ensemble des documents transmis dans un CPD et non sur chaque document individuellement.

La signature doit être faite en utilisant le standard PKCS#7 (algorithme SHA1) sur base du fichier en clair, non zippé. Cette signature doit être incluse en texte encodé base64 dans le CPD ainsi que le certificat utilisé pour signer.

Le signataire peut être le prestataire individuel ou le responsable de groupement ainsi que tout utilisateur MyCareNet autorisé par ceux-ci via « user management » (voir site de la sécurité sociale) ou via « mandat » (voir Convention MyCareNet Infirmiers).

Contraintes sur les systèmes informatiques des prestataires et des OAs

Il est demandé aux systèmes informatiques des prestataires et des OAs de prévoir ce qui suit :

Description des données à archiver
Voir art 6 du protocole

Description de la procédure d'archivage
Journalièrement, l'ensemble des fichiers cités dans la partie « description des données à archiver » sera sauvé en deux exemplaires distincts sur support non volatile. Ces fichiers sauvegardés pourront être joints à ceux sauvés antérieurement mais devront, par la suite, pouvoir en être isolés.

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 dupliquées 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.

Description de la procédure de recherche dans l'archivage et de publication des archives
Concernant la recherche dans l'archivage, l'accès pourra se faire en mentionnant différents critères de recherche dont au moins les critères suivants isolément ou combinés : sender, receiver, type de message, date de création du message.
Concernant la publication des archives, se référer à art 7 du protocole.

Description des moyens informatiques logiciels et matériel mis en oeuvre
Le matériel, les logiciels, et les 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 du prestataire ou de l'O.A. de faire le nécessaire pour récupérer les informations sur un nouveau support.

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

Procédure d'adhésion d'un fournisseur de logiciel dans MyCareNet

Pour autoriser un logiciel à utiliser MyCareNet, un ensemble de démarches administratives sont à réaliser ainsi qu'un ensemble de tests techniques et business avec la plateforme MyCareNet et avec les OAs.

La procédure complète d'adhésion d'un fournisseur de logiciel est décrite dans le document « MyCareNet vademecum » disponible auprès du collège intermutualiste national (CIN).