Protocol, opgemaakt op 17 maart 2010 door de Overeenkomstencommissie verpleegkundigen - verzekeringsinstellingen, houdende de voorwaarden en modaliteiten volgens welke bewijskracht kan worden gegeven tot het bewijs van het tegendeel aan gegevens die worden opgeslagen of bewaard door middel van een elektronische techniek of medegedeeld op een andere wijze dan op een papieren drager, evenals de voorwaarden en modaliteiten volgens welke deze gegevens worden weergegeven op papieren drager of op elke andere leesbare drager.

Gelet op artikel 9bis van de wet betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen, gecoördineerd op 14 juli 1994;
Gelet op het koninklijk besluit van 27 april 1999, gewijzigd bij het koninklijk besluit van 26 april 2007, betreffende de bewijskracht van de door de zorgverleners, de verzekeringsinstellingen, het Rijksinstituut voor ziekte- en invaliditeitsverzekering en andere natuurlijke of rechtspersonen met toepassing van gecoördineerde wet van 14 juli 1994 en haar uitvoeringsbesluiten opgeslagen, verwerkte, weergegeven of meegedeelde gegevens;
Gelet op het voorstel van protocol, opgemaakt door de Overeenkomstencommissie verpleegkundigen - verzekeringsinstellingen, bedoeld in artikel 17 van het koninklijk besluit van 3 juli 1996 tot uitvoering van de wet betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen, gecoördineerd op 14 juli 1994;
Gelet op het advies van het Comité van de Dienst voor Administratieve Controle van het Rijksinstituut voor ziekte- en invaliditeitsverzekering, uitgebracht op 29 maart 2010;
Gelet op het advies van het Comité van de Dienst voor Geneeskundige Evaluatie en Controle van het Rijksinstituut voor ziekte- en invaliditeitsverzekering, uitgebracht op 26 maart 2010;
Gelet op het advies van het Comité van de verzekering voor geneeskundige verzorging van het Rijksinstituut voor ziekte- en invaliditeitsverzekering, uitgebracht op 29 maart 2010;
Gelet op de goedkeuring, gegeven door de Minister van Sociale Zaken op 21 juni 2011,

Artikel 1. § 1. Voor de toepassing van dit protocol wordt verstaan onder:

1° "RIZIV": het Rijksinstituut voor ziekte- en invaliditeitsverzekering zoals bedoeld in artikel 10 van de wet betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen, gecoördineerd op 14 juli 1994;
2° “nomenclatuur” : de bijlage bij het koninklijk besluit van 14 september 1984 tot vaststelling van de nomenclatuur van de geneeskundige verstrekkingen inzake verplichte verzekering voor geneeskundige verzorging en uitkeringen;
3° "protocol" : het protocol zoals bedoeld in artikel 2 van het koninklijk besluit van 27 april 1999, gewijzigd bij het koninklijk besluit van 26 april 2007, betreffende de bewijskracht van de door de zorgverleners, de verzekeringsinstellingen, het Rijksinstituut voor ziekte- en invaliditeitsverzekering en andere natuurlijke of rechtspersonen met toepassing van gecoördineerde wet van 14 juli 1994 en haar uitvoeringsbesluiten opgeslagen, verwerkte, weergegeven of meegedeelde gegevens;
4° "zorgverleners”: de zorgverleners bedoeld in artikel 21quater van het Koninklijk Besluit nr. 78 betreffende de uitoefening van de gezondheidszorgberoepen – 10.11.1967 – MB 14.11.1967 (W. 10.08.1967), en de groeperingen van deze zorgverleners;
5° "verzekeringsinstellingen": de instellingen bedoeld in artikel 2, i), van de hier voren genoemde wet van 14 juli 1994.

Art. 2. De bijlage 1 « MyCareNet : Overeenkomst tussen verzekeringsinstellingen en verpleegkundigen » en de bijlage 2 « MyCareNet : Technische principes van uitwisseling en reproductie van de gegevens», evenals hun latere wijzigingen, moeten goedgekeurd worden door de Overeenkomstencommissie verpleegkundigen - verzekeringsinstellingen bedoeld in artikel 17 van het koninklijk besluit van 3 juli 1996 tot uitvoering van de hier voren genoemde wet van 14 juli 1994.

Art. 3. Dit protocol omschrijft de procedure waaraan moet worden voldaan opdat, in uitvoering van het hier voren genoemde koninklijk besluit van 27 april 1999, bewijskracht kan worden gegeven aan de hierna opgesomde elektronisch meegedeelde, opgeslagen, verwerkte of weergegeven gegevens:
- gegevens inzake facturatie ;

- medisch-administratieve documenten, met name de aanvragen van toiletten en forfaits, de kennisgevingen van de palliatieve zorgen en de aanvragen van de specifieke technische verpleegkundige verstrekkingen.

Het versturen van deze gegevens tussen zorgverleners of binnen de verzekeringsinstelling valt buiten de toepassing van dit protocol.

Art. 4. De vertegenwoordiging van de zorgverleners en, in voorkomend geval, de identificatie van de volmachthouders zijn bepaald in bijlage 1 « MyCareNet : Overeenkomst tussen verzekeringsinstellingen en verpleegkundigen » van dit protocol.

Art. 5. In uitvoering van artikel 3 en artikel 9, 1° en 5° van het hier voren genoemde koninklijk besluit van 27 april 1999, moet de gegevensuitwisseling verlopen conform aan de principes van MyCareNet zoals bepaald in bijlage 2 « MyCareNet : Technische principes van uitwisseling en reproductie van de gegevens » van dit protocol.

Art. 6. In uitvoering van artikel 9, 2°, 3° en 4° van het hier voren genoemde koninklijk besluit van 27 april 1999, moeten de door de zorgverleners en door de verzekeringsinstellingen gebruikte informaticasystemen er voor instaan dat de uitgewisselde gegevens systematisch en volledig bewaard worden, dat de integriteit en de authenticiteit ervan gegarandeerd wordt en dat het vertrouwelijk karakter beschermd wordt. Bovendien moeten gegevens betreffende de identiteit van de verantwoordelijke voor het versturen evenals van diegene die de verzending heeft uitgevoerd , een volledige tijdsinformatie en de rapporten van de eventuele storingen die zijn vastgesteld tijdens de verwerking bewaard worden.

De bewaringstermijn van de uitgewisselde gegevens en de hieraan gekoppelde verzendingsrapporten is dezelfde als diegene die geldt voor het verpleegdossier in artikel 8 van de nomenclatuur van de geneeskundige verstrekkingen.

Art. 7. In uitvoering van artikel 9, 1° van het hier voren genoemde koninklijk besluit van 27 april 1999, moet de verstuurde of ontvangen informatie getrouw kunnen weergegeven worden op een leesbare papieren drager, met identificatie van de persoon die de originele informatie verstuurd heeft en identificatie van de persoon die verantwoordelijk is voor het afdrukken.

De Dienst voor Geneeskundige Evaluatie en Controle of de Dienst voor Administratieve Controle moeten – op hun vraag – toegang hebben tot deze gegevens door het afdrukken van deze gegevens op papieren drager, zoals hierboven vermeld, door consultatie van de gegevens op het computerscherm, een terminal of een werkstation of door het ter beschikking stellen van de gegevens op een elektronische drager.

Art. 8. Het toezicht op het respecteren van de bepalingen van dit protocol en zijn bijlagen gebeurt door respectievelijk de Dienst voor Geneeskundige Evaluatie en Controle en door de Dienst voor Administratieve Controle, elk op vlak van hun bevoegdheden.

Onverminderd hun eigen specifieke bevoegdheden zullen de Controlediensten eventuele onregelmatigheden of tekortkomingen meedelen aan de Overeenkomstencommissie verpleegkundigen - verzekeringsinstellingen bedoeld in artikel 17 van het koninklijk besluit van 3 juli 1996 tot uitvoering van de hier voren genoemde wet van 14 juli 1994.

Bijlage 1

MyCareNet – Overeenkomst tussen verzekeringsinstellingen en verpleegkundigen.

Doel

Het doel van deze overeenkomst is de praktische en dwingende werkregels, complementair aan de regelgeving, vast te leggen voor de elektronische gegevensuitwisseling via het MyCareNet-netwerk tussen verpleegkundigen en verzekeringsinstellingen.

Definities

- **Verzekeringsinstelling**: de instellingen bedoeld in artikel 2,i) van de wet van 14 juli 1994
- **Zorgverlener**: de zorgverleners bedoeld in artikel 21quater van het van het Koninklijk Besluit nr. 78 in relatie met de uitoefening van de gezondheidszorgberoepen – 10.11.1967 – MB 14.11.1967 (L. 10.08.1967), en de groeperingen van deze zorgverleners.
- **Netwerk**: het netwerk MyCareNet.
- **Service**: type van gegevensuitwisseling (verzekerbaarheid, facturatie, medisch-administratief luik) waartoe de zorgverlener wenst toe te treden.
- **Volmacht**: is een juridische handeling tussen twee geïdentificeerde entiteiten waarbij de ene entiteit (volmachtgever) de andere entiteit (volmachthouder) gedurende een welbepaalde termijn toelaat toegang te hebben tot het MyCareNet netwerk en dit in naam van de mandaatgever voor één welbepaalde service.
- **Volmachtgever**: geïdentificeerde entiteit die mandaat geeft.
- **Volmachthouder**: geïdentificeerde entiteit die mandaat krijgt om toegang te hebben tot het netwerk MyCareNet en dit in naam van de volmachtgever voor één welbepaalde service.

Rechten en plichten van de partijen

- **Rechten en plichten van de verzekeringsinstellingen**
  - Beschikbaarheid van de diensten:
    - Op technisch niveau (beschikbaarheid van het netwerk MyCareNet)
      - Aanvragen kunnen in principe door de zorgverleners 24 uur op 24 worden ingebracht, buiten de kantooruren wordt hierop door de verzekeringsinstellingen gereageerd naar best effort.
    - Op het niveau van de MyCareNet Helpdesk
      - de helpdesk zal minstens ter beschikking zijn tijdens de kantooruren van 8 uur tot 18 uur en dit alleen op werkdagen. In een apart document wordt vermeld tot wie de zorgverlener zich kan wenden met welke vragen.
    - Op het niveau van de helpdesks van de verzekeringsinstelling
      - de helpdesk zal ter beschikking zijn tijdens de kantooruren van 9 uur tot 12 uur en van 13u30 tot 16 uur en dit alleen op werkdagen. In een apart document wordt vermeld waar de zorgverlener zich kan wenden met welke vragen.
    - De coördinatie tussen de helpdesks van MyCareNet en de VI wordt verzekerd.

Rechten en plichten van de zorgverleners:

- De zorgverleners zijn verantwoordelijk voor de juistheid en het up-to-date zijn van hun gegevens in de authentieke bronnen (Bijvoorbeeld : als verantwoordelijke van een groepering t.o.v. het RIZIV, als verantwoordelijk bestuurder t.o.v. de Kruispuntbank der Ondernemingen, …)
- De eventuele toekomstige aanpassingen aan deze overeenkomst zullen goedgekeurd worden door de Overeenkomstencommissie van de Verpleegkundigen. De meest actuele versie van deze overeenkomst kan ten alle tijden opgevraagd worden aan de coördinatiecel van het Nationaal Intermutualistisch College.
- Een zorgverlener heeft recht op toegang tot het netwerk mits e-Health de identiteit en de hoedanigheden die de zorgverlener aanbrengt heeft erkend en goedgekeurd.
- Het gebruik maken van dit netwerk voor een service (verzekerbaarheid , facturatie, medisch administratief luik) houdt de automatische aanvaarding in van de voorwaarden bepaald in de bijlage met betrekking tot deze service.
- De helpdesk eerste lijn voor de zorgverlener is altijd de leverancier van het softwarepakket waarmee de zorgverlener MyCareNet aanroept (dus in geval van problemen met MyCareNet zal de zorgverlener zijn leverancier contacteren).
- De zorgverlener verbindt er zich toe regelmatig de berichten (antwoorden) in de mailbox op te vragen zodat hij op de hoogte is van de communicatie vanuit de verzekeringsinstellingen (akkoord, weigering, aanpassing forfait door de adviserende geneesheer).
- De, voor de prestatieverlener, ter beschikking gestelde gegevens kunnen gedurende maximum drie maanden opgevraagd (gedownload) worden bij (van) MycareNet.
- In geval van misbruik of inbreuk op de huidige overeenkomst :
  - Zodra een verzekeringsinstelling misbruiken of overtredingen van de bepalingen van deze overeenkomst vaststelt, zal ze aan de zorgverlener per aangetekend schrijven een verwittiging hierover verzenden.
  - Bij herhaling van de feiten binnen de 365 dagen, zal dit ter kennis worden gebracht van de Overeenkomstencommissie verpleegkundigen en de administratieve en medische controlediensten van het RIZIV die, elk volgens hun bevoegdheden en respectievelijke verantwoordelijkheden, de nodige acties zullen ondernemen ten aanzien van de zorgverlener.
  - Het NIC zal alle zich aangaande gevallen van misbruik overmaken aan het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid dat toeziet op de veiligheid en op de bescherming van het privé-leven van de sociaal verzekerden voor de betrokken service.
- Indien het gebruik van het netwerk door de zorgverlener de beschikbaarheid of de veiligheid van het informaticasysteem in gevaar brengt, kan de zorgverlener tijdelijk de toegang tot het informaticasysteem ontzegd worden, totdat het probleem opgelost is (het betreft hier problemen van technische aard).

Vertegenwoordiging

Wanneer de zorgverlener een natuurlijk persoon is, treedt hij/zij zelf op.
Wanneer de zorgverlener een rechtspersoon is, wordt hij/zij vertegenwoordigd door een persoon die hiertoe werd aangeduid in de statuten van deze rechtspersoon.
Wanneer de zorgverlener een feitelijke vereniging is, treedt de vertegenwoordiger die de vereniging aan het RIZIV heeft meegedeeld ook binnen deze overeenkomst op als vertegenwoordiger.
De zorgverlener blijft steeds aansprakelijk voor de handelingen van de personen die hij/zij aanduidt.
De verzekeringsinstellingen zullen enkel rekening houden met documenten die ondertekend worden door de wettelijke vertegenwoordiger van een zorgverlener of door een aangestelde die hiertoe gemachtigd werd. Dit geldt niet voor de elektronische documenten die hun eigen regels hebben.
Aan de gegevens die via het netwerk worden uitgewisseld kan bewijskracht worden verleend conform art.9 bis W 14.7.94 (modaliteiten gedefinieerd in een protocol bewijskracht).

Volmachten

Een zorgverlener heeft het recht een volmacht te geven aan een volmachthouder.
Een volmacht moet schriftelijk bevestigd worden volgens het model op het platform e-health.
(https://www.ehealth.fgov.be/nl/page_menu_a_m/website/home/portal/access/mandates.html)
De volmachtgever dient deze volmacht ter kennis te brengen bij het Nationaal Intermutualistisch College. De periode voor de welke de volmacht werd verleend moet uitdrukkelijk vermeld zijn in deze volmacht. De volmacht moet minstens vijf werkdagen voor de datum van ingang van de volmacht afgeleverd worden aan het NIC.
De volmachtgever blijft aansprakelijk voor de inhoud van de berichten en meer specifiek voor de inhoud van de facturatie en de effectiviteit van de geleverde prestaties. Zorgverleners wiens verstrekkingen geattesteerd worden via een groepsnummer (zoals bedoeld op de website van het Riziv www.riziv.fgov.be) moeten geen volmacht MyCareNet geven.

Teneinde geldig te zijn, moeten de volmachten aan de volgende limitatief opgesomde voorwaarden voldoen:

- De volmacht moet uitdrukkelijk vermelden wat het voorwerp is van de volmacht. Een volmacht geldt enkel voor maximaal 1 service (verzekerbaarheid, facturatie, medisch-administratief luik).
- Een volmacht zal niet slaan op de betalingswijze. Hiervoor moet er een specifiek akkoord tussen de zorgverlener en de verzekeringsinstelling worden afgesloten.
- De datum van de ondertekening moet uitdrukkelijk vermeld worden zodat de betrokken verzekeringsinstelling kan nagaan wanneer deze volmacht uitwerking zal hebben.
- Er mogen geen overlappende periodes bestaan tussen twee volmachten voor een zelfde service. In dat geval zal een nieuwe volmacht automatisch de bestaande volmacht afsluiten.
- Bij het overlijden, het faillissement of de vereffening van de volmachtgever of de volmachthouder wordt elke volmacht onmiddellijk beëindigd. Een nieuwe volmacht kan eventueel afgesloten worden door of met de vereffenaar of de curator.

Evaluatie

Een voortdurende evaluatie van deze overeenkomst zal uitgevoerd worden.

Bijlage service Facturatie

Doel

Het doel van deze bijlage is de praktische en dwingende werkregels vast te leggen voor de elektronische gegevensuitwisseling in de service facturatie.

Definities

Facturatie is het overmaken van de facturen en het antwoord hierop op administratief vlak tussen de zorgverleners en de verzekeringsinstellingen via elektronische weg en dit in de derdebetalersregeling.

Rechten en plichten van de partijen

- **Rechten en plichten van de verzekeringsinstellingen**

    - De verzekeringsinstellingen verbinden zich ertoe de facturen te behandelen binnen de termijn zoals bepaald in de overeenkomsten tussen verzekeringsinstellingen en betrokken zorgverleners.
    - De facturen worden slechts als ontvangen beschouwd op het ogenblik van de ontvangstmelding door de verzekeringsinstelling via het netwerk.
    - De VI zijn gehouden tot een betalingsverbintenis conform de voorwaarden van art.159 bis KB 3.7.96 gewijzigd door het KB van 5 juni 2008

- **Rechten en plichten van de zorgverleners**:

    - De zorgverlener verbindt zich ertoe geen magnetische dragers meer over te maken aan de verzekeringsinstellingen eens hij de facturatiebestanden verstuurt via MyCareNet.
    - De zorgverlener zal de ontvangen gegevens strikt vertrouwelijk behandelen.

Bijlage service Verzekerbaarheid

Doel

Het doel van deze bijlage is de praktische en dwingende werkregels vast te leggen voor de elektronische gegevensuitwisseling in de service verzekerbaarheid.

Definities

Verzekerbaarheid: de bevestiging van gegevens voor het verifiëren van het recht op terugbetaling door de ziekte- en invaliditeitsverzekering, evenals de gegevens over het toe te passen terugbetalingstarief, statuut en de periode voor de welke deze gegevens gelden. Deze raadpleging gebeurt online voor één patiënt of met uitgestelde verwerking voor een lot van één of meerdere patiënten.

Rechten en plichten van de partijen

- **Rechten en plichten van de verzekeringsinstellingen**

    - De verzekeringsinstellingen verbinden zich ertoe steeds de meest actueel beschikbare informatie te verstrekken.
    - Antwoorden in de service verzekerbaarheid worden bezorgd binnen de eerstvolgende werkdag na de aanvraag en dit voor 95 % van de aanvragen. Dit percentage wordt berekend op het geheel van de aanvragen (verzekerbaarheid online + verzekerbaarheid met uitgestelde verwerking).
    - De verzekeringsinstellingen zijn gehouden de gegevens ter beschikking te stellen van de zorgverleners die zij nodig hebben om de prestaties correct te kunnen factureren.

- **Rechten en plichten van de zorgverleners**:

    - De zorgverlener verbindt er zich toe enkel gegevens op te vragen en te verwerken voor de patiënten die hij effectief behandelt en dit met als enige finaliteit de facturatie van geneeskundige behandelingen.
    - De zorgverlener verbindt er zich toe om voor minimaal 99 % van de patiënten waarvoor hij/zij de gegevens in verband met de verzekerbaarheid heeft opgevraagd, effectief over te gaan tot een facturatie.
    - De zorgverlener zal de ontvangen gegevens strikt vertrouwelijk behandelen en niet overdragen aan andere zorgverleners of aan derden.
    - De basisregel is de volgende : de zorgverlener kan voor éénzelfde behandeling van een patiënt de gegevens in verband met de verzekerbaarheid slechts éénmaal informatief opvragen bij het begin van de behandeling en daarna met het oog op de facturatie maximaal éénmaal per maand. Er kunnen uitzonderingen gemaakt worden voor speciale situaties (bvb. Een patiënt die niet in regel is en waarvoor men de verzekerbaarheid heropvraagt).

Bijlage Medisch-administratieve luik

Doel

Het doel van deze bijlage is de praktische en dwingende werkregels vast te leggen voor de elektronische gegevensuitwisseling voor het medisch-administratieve luik.

Definities

Medisch-administratieve luik: Het betreft het elektronisch verzenden van de kennisgevingen en de aanvragen van de zorgverstrekker aan de verzekeringsinstelling betreffende de te verstrekken verpleegkundige zorgen bij de patiënt en de elektronische antwoorden van de verzekeringsinstelling hierop. De richtlijnen uit artikel 8 van de nomenclatuur gelden als wettelijke basis voor deze elektronische uitwisselingen. Binnen het medisch-administratieve luik worden drie domeinen onderscheiden. De aanvragen toiletten en forfaits A, B en C gebeuren via de berichten 410XXX. De kennisgevingen palliatieve zorgen gebeuren via de berichten 420XXX. De kennisgevingen van de specifieke technische verpleegkundige verstrekkingen verlopen via de berichten 430XXX.

Rechten en plichten van de partijen

- **Rechten en plichten van de verzekeringsinstellingen**
    - De verzekeringsinstellingen verbinden zich ertoe steeds de meest actueel beschikbare informatie te verstrekken (De uitgewisselde informatie is beschreven in de MyCareNet berichten).
    - De verzekeringsinstellingen verbinden zich ertoe de antwoorden in het medisch-administratieve luik ter beschikking te stellen binnen een redelijke termijn.
    - De kennisgevingen en aanvragen worden pas beschouwd als zijnde toegekomen in de VI als MyCareNet een verzendbewijs ter beschikking heeft gesteld van de verstrekker met daarin datum en uur waarop MyCareNet het corresponderende bericht ontvangen heeft. In geval van conflict, is het aan de verstrekker aan te tonen dat hij beschikt over het verzendbewijs. Het verzendbewijs is geen akkoord van de VI voor een financiële tussenkomst bij gevraagde zorgen binnen de ZIV.
    - De verzekeringsinstellingen verbinden zich ertoe om voor elke kennisgeving en aanvraag een antwoord ter beschikking te stellen van de aanvragende verstrekker. Dit antwoord kan een verwerping zijn (bericht kan niet behandeld worden – formaatfouten – etc.), een ontvangstbewijs zijn (bewijs dat de VI het bericht goed ontvangen en ingeschreven heeft – voorbeeld : ontvangstbewijs voor een kennisgeving specifieke technische prestatie), een aanvaarding zijn (aanvraag goedgekeurd door de adviserende geneesheer) of een weigering zijn (aanvraag geweigerd door de adviserende geneesheer). Het is dit antwoord dat de financiële tussenkomst bij gevraagde zorgen binnen de ZIV bepaalt.
    - De aanpassing van een forfait, naar aanleiding van een beslissing van een adviserend geneesheer, wordt beschouwd in te gaan vanaf de dag dat de verzekeringsinstelling de verstrekker ervan inlicht.

- **Rechten en plichten van de zorgverleners**:

    - De zorgverlener verbindt er zich toe zich eerst te vergewissen van de mutualistische aansluiting van zijn patiënt alvorens een kennisgeving of aanvraag elektronisch te verzenden. Zo kan de zorgverstrekker de kennisgeving of de aanvraag steeds naar de juiste verzekeringsinstelling verzenden.
    - De zorgverlener zal de ontvangen gegevens strikt vertrouwelijk behandelen en enkel overdragen aan andere zorgverleners om de continuïteit van de zorg te waarborgen.
    - De zorgverlener staat garant voor het bewaren in het dossier van de patiënt van alle attesten, voorschriften, behandelingsplannen, … omschreven in de nomenclatuur waarvoor het gebruik van MyCareNet hen toestaat deze niet meer aan de verzekeringsinstelling te moeten overmaken. Deze documenten moeten ter beschikking gehouden worden van de adviserend geneesheer naar aanleiding van een bezoek of op eenvoudig verzoek. Deze documenten moeten ook ter beschikking gehouden worden van de Dienst voor Geneeskundige Evaluatie en Controle, voor wat zijn bevoegdheden betreft.

Bijlage 2 : Oplossing MyCareNet : Technische principes van uitwisseling en reproductie van de gegevens

Inleiding

MyCareNet is een oplossing uitgewerkt door de verzekeringsinstellingen voor de beveiligde uitwisseling van gestructureerde informatie met de zorgverstrekkers via het internet.

MyCareNet is een evolutie van de CareNet oplossing die sinds meerdere jaren operationeel is voor de uitwisselingen met de ziekenhuissector.

Vanuit een informatica oogpunt bestaat de MyCareNet oplossing uit :

- De infrastructuur componenten en meer bepaald het informatica platform die de uitwisselingen coördineert. Dit uitwisselingsplatform wordt beheerd door het Nationaal Intermutualistisch College (NIC) in naam van de verzekeringsinstellingen (VI).
- Informatica verwerking van de informatie eigen aan elke bijzondere toepassing (vb : verzekerbaarheid) zowel bij de zorgverstrekker, als bij elke VI alsook op het MyCareNet platform.
- Externe informatica diensten die voornamelijk geleverd worden door het eHealth platform.

De MyCareNet oplossing integreert eveneens :

- De governance diensten en procedures : helpdesk, service management, evolutie en correctie onderhoud, beheer van de aansluitingen en van de testen, capacity management, etc.
- Regelgeving die de organisatie en het gebruik ervan bepalen in functie van de wetgeving en voornamelijk de onderrichtingen van de toezichthouders alsook de eisen van het respect op de privacy.

Het bovenstaand schema geeft een algemeen beeld van de architectuur van het netwerk en van zijn belangrijkste componenten :

- het telecommunicatie netwerk: Internet, rekening houdend met zijn algemene karakter, met zijn lage gebruikskost, met de al bestaande technieken die de mededelingen en de meegedeelde informatie met de noodzakelijke beveiliging kunnen dekken;

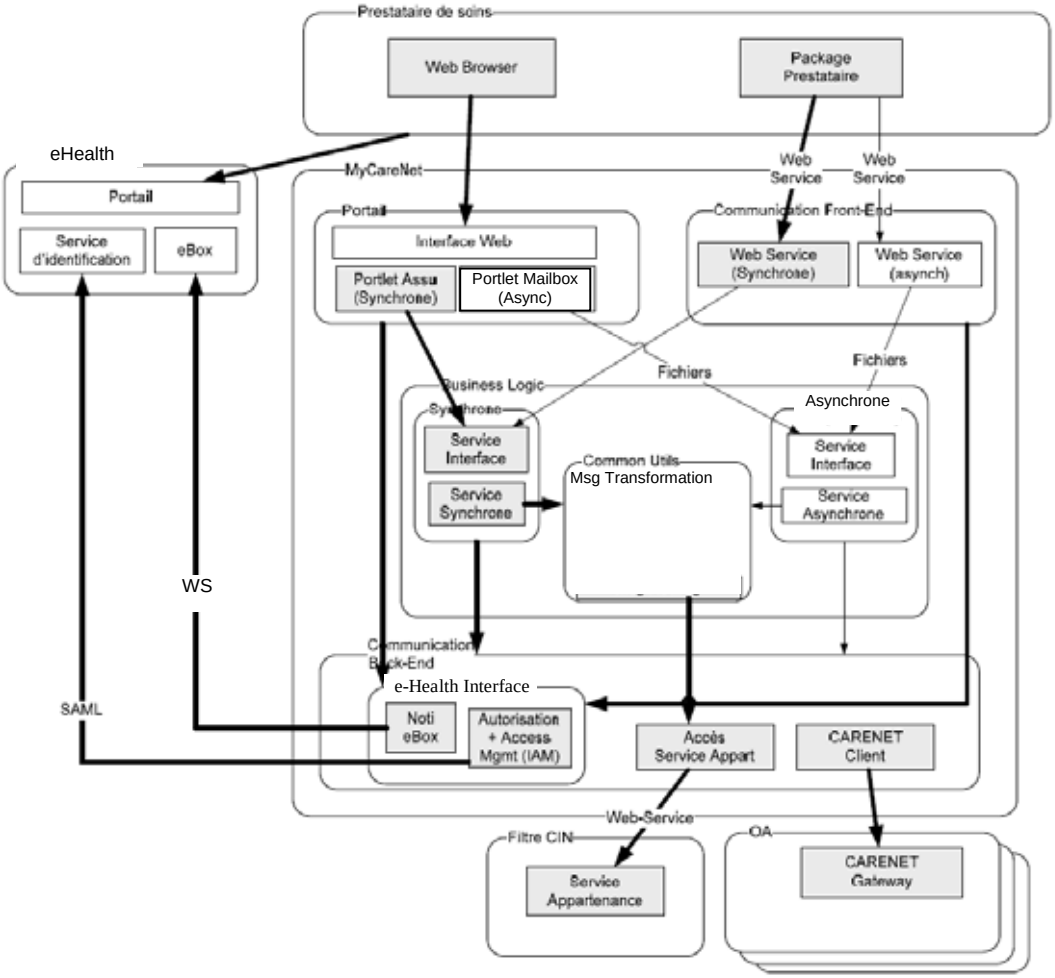
- de werkplaats van de zorgverstrekker: het is de zorgverstrekker die, vanuit zijn werkplaats, via het portaal of via de toepassing, verschillende communicaties tot stand brengt naar de verzekeringsinstellingen toe;

- eHealth portaal : deze geeft de mogelijkheid om zich aan te sluiten met verschillende eHealth portalen van de sector gezondheidszorg;

- MyCareNet portaal : gecreëerd en beheerd door het NIC. Dit portaal laat toe, naast complexe gebruikersfuncties, de verbinding tussen de zorgverstrekker en de verzekeringsinstelling te maken in functie van de mutualistische aansluiting van de patiënt. Het MyCareNet portaal stelt, op basis van het profiel van de zorgverstrekker, verschillende functionaliteiten voor, die door de zorgverstrekker gekozen worden in functie van de noden van het moment.

Beschrijving van de stromen (encryptie methode inbegrepen)

Logische architectuur



Standaard beschikt MyCareNet over 2 interfaces die de zorgverstrekker toelaten om hun toepassingen aan te roepen.

- Systeem naar systeem
  In dit geval, dient de toepassing van de gebruiker in staat te zijn om beroep te doen op « web services », dit is een technologie die toelaat om met een standaard te communiceren, onafhankelijke van de taal en de ontwikkelingstools van de client en server toepassingen. Deze communicatie laat een maximale integratie van diensten en uitgewisselde gegevens toe. De applicatie van de gebruiker moet ook in staat zijn de verschillende uitgewisselde berichten te visualiseren.

- Het portaal
  In dit geval sluit de gebruiker zich onmiddellijk aan op het protaal (website) van MyCareNet die zijn diensten, door middel van HTML pagina's aanbiedt.
  MyCareNet werkt met elektronische formulieren van aanvragen die men invult en visualisatie van de antwoorden en/of via opladen/afhalen van bestanden.
  Hoewel de integratie minder nadrukkelijk is, laat deze oplossing de gebruikers toe om beroep te doen op de voornaamste diensten met een minimum aan ontwikkeling van applicaties. Deze oplossing is ook nuttig als de toepassing niet compatibel is met de technologie van webservices.

Wat betreft de mogelijke manieren van werken, laat MyCareNet de volgende uitwisselingen toe :

- Online, ook synchroon genoemd :
  In dit geval geeft MyCareNet een antwoord aan een unieke vraag in een aanvaardbare termijn van enkele seconden die compatibel is met de praktische werking bij de zorgverstrekker.

- « Batch » ook « asynchroon » of « uitgesteld » genoemd :
  Eén of meerdere vragen worden in een lot verstuurd naar MyCareNet die de routing verzekerd naar de verschillende bestemmingen.
  De antwoorden op de aanvragen worden voorbereid in een afgesproken termijn van enkele uren of dagen (volgens de diensten).
  De gebruiker dient zijn « mailbox » te raadplegen om het verloop van verwerking op te volgen en de antwoorden te behandelen.
  Dit wordt voornamelijk toegepast bij werkmethodes die een menselijke tussenkomst vereisen. (voorbeeld de toestemming van een adviserend geneesheer)
  De batch oplossingen laten, in sommige gevallen toe dat de verzekeringsinstellingen op eigen initiatief informatie versturen (zonder voorafgaande vraag).

MyCareNet platform bevat een « business logic » bloc die 3 modules inhoud :

- *Synchrone module*

Behandeld de aanvragen (inbound) en de antwoorden (outbound) op welke de aanvrager een onmiddellijk antwoord verwacht (synchroon).

- *Asynchrone module*

Behandeld de asynchrone aanvragen (batch). Het interne statuut van de aanvragen is beschikbaar via de opvolging van het statuut van de berichten.

- *Module "Gemeenschappelijke hulpprogramma's"*

Bevat functies voor het behandelen van de berichten die gebruikt kunnen worden zowel door de synchrone als asynchrone module.

Het MyCareNet platform gebruikt de volgende basis diensten van eHealth :

- Portaal site
- Geïntegreerd beheer van de gebruikers en toegangen (mandaten inbegrepen)
- Beveiligde elektronische mailbox (eBox)

Deze diensten zijn gedocumenteerd op www.ehealth.fgov.be.

Het MyCareNet platform maakt eveneens gebruik van de NIC filter van de mutualistische aansluitingen.

Om met de VI te communiceren wisselt MyCareNet berichten uit met een Client gateway via het CareNet netwerk. Bij de verzekeringsinstellingen bevindt zich een gateway Server. Deze gateways nemen het tekenen en vercijferen van de informatie die verstuurd wordt via het netwerk op zich en dit met behulp van specifieke certificaten.
Het document “carenet user’s guide « administration and programming »” beschrijft volledig de functionaliteiten van de gateways en is beschikbaar op www.mycarenet.be.

Beschrijving van de stromen

De verschillende stromen die via MyCareNet gecommuniceerd worden staan in het document « MyCareNet – Care Provider Implementation Guide » beschreven, die enkel in het Engels beschikbaar is, bij het Nationaal Intermutualistisch College (NIC).

In de beschrijving van de facturatie en medisch-administratieve stromen moet benadrukt worden dat de getekende informatie, zoals ontvangen van de prestatieverlener, ook naar de VI verstuurd wordt om te dienen voor integriteitcontroles, en omgekeerd.

Inhoud en formaat van de berichten (inbegrepen ontvangstbewijs en foutieve berichten)

De inhoud en het formaat van de berichten aanwezig in de stromen die via MyCareNet gecommuniceerd worden en die goedgekeurd werden door de commissie van de elektronische berichten en door het verzekeringscomité gezondheidszorgen, worden gepubliceerd op de site : **www.mycarenet.be**.

De bestanden verstuurd in de facturatie berichten respecteren de lay-out zoals voorgeschreven in de “Instructies facturatie via magnetische of elektronische drager” dewelke beschikbaar zijn op de site www.riziv.be .

Encryptie methode

Er is een encryptie, op basis van SSL/TLS, gerealiseerd conform de machtigingen n°07/070 van 04/12/07 en n° 07/003 van 09/01/07 tussen de verstrekkers en MyCareNet indien dit vereist is door het Sectoraal comité van de Sociale Zekerheid en van de gezondheidszorg - afdeling “sociale zekerheid”. Tussen MyCareNet en de VI’s wordt de encryptie uitgevoerd in CareNet met triple DES encryptie op basis van een 128bits sleutel zoals op de site www.mycarenet.be beschreven.

Identificatie, authenticatie en toelating van de zorgverstrekkers

Ter herinnering,

De **authenticatie** is de procedure die, voor een informatica systeem, bestaat uit de identificatie van een entiteit (persoon, computer…) na te kijken teneinde deze entiteit toegang te verlenen aan bronnen (systemen, netwerken, toepassingen…). De authenticatie laat dus het valideren van de authenticiteit van de betrokkenen entiteit toe.

De **identificatie** laat toe de identiteit van een entiteit te kennen maar de **authenticatie** laat toe om de identiteit te verifiëren.

In het geval van interacties systeem naar systeem

Alvorens beroep te doen op de functionele webservices van MyCareNet of van eHealth moet er eerst een sessie MyCareNet geopend worden.

In de praktijk dient de gebruiker zich eerst te identificeren en te authenticeren als persoon door middel van zijn identificatiegegevens bij het rijksregister op zijn elektronische identiteitskaart. [1]

Dankzij het authenticatie certificaat (beschermd door de pincode), zal hij een openingsaanvraag ondertekenen die hij onder vorm van een bijzondere webservice naar MyCareNet overmaakt.

MyCareNet zal het identificatienummer bij het rijksregister van de gebruiker authenticeren, namelijk door de uitvoering van een validiteitcontrole van het certificaat.

MyCareNet zal antwoorden op de openingsaanvraag van de sessie die gemanifesteerd wordt door een sleutelpaar en dit voor de duur van de sessie of een gelijkwaardige techniek.[2]

Elke aanvraag via webservice zal door middel van een privé sleutel ondertekend worden, dewelke de authenticiteit en de integriteit waarborgt.

De sessie stemt dus overeen met de periode waarin de identificatie en de authenticatie van de gebruiker als persoon voor MyCareNet geldig blijven.

De sessie kan opgesteld worden voor een bepaalde duur door de aanvraag maar kan een maximum niet overschrijden. Dit maximum wordt tegenwoordig vastgelegd op 12 uur (ook de default waarde) en kan herzien worden.

Een bijzondere webservice laat de gebruiker toe om voorafgaandelijk zijn sessie te sluiten, voornamelijk als hij definitief zijn werkplaats verlaat.

Een sessie kan niet verlengd worden maar wel heropend worden. Dit wil in de praktijk zeggen een herlezing van de identiteitskaart.

[1] Andere mogelijkheden worden bestudeerd, zoals bijvoorbeeld de Fedict certificaten

[2] De techniek voor het openen van een sessie, momenteel gebaseerd op het XKMS protocol, is in detail beschreven in het document “MyCareNet – Care Provider implementation Guide”.

Wat de controle van de autorisaties betreft, zal de gebruiker in eerste instantie de zorgverstrekker (nummer RIZIV) identificeren waarvoor hij wenst te werken alsook de rol dat hij wil spelen (voorbeeld in geval van mandaat).
Dit zal gecodeerd worden in een structuur “sender” genoemd.

De gebruiker zal ook het type aanvraag aanduiden dat hij wil opsturen (voorbeeld een aanvraag van de rechten van de patiënt, …).

Elk beroep op een functionele webservice zal deze 2 elementen bevatten.

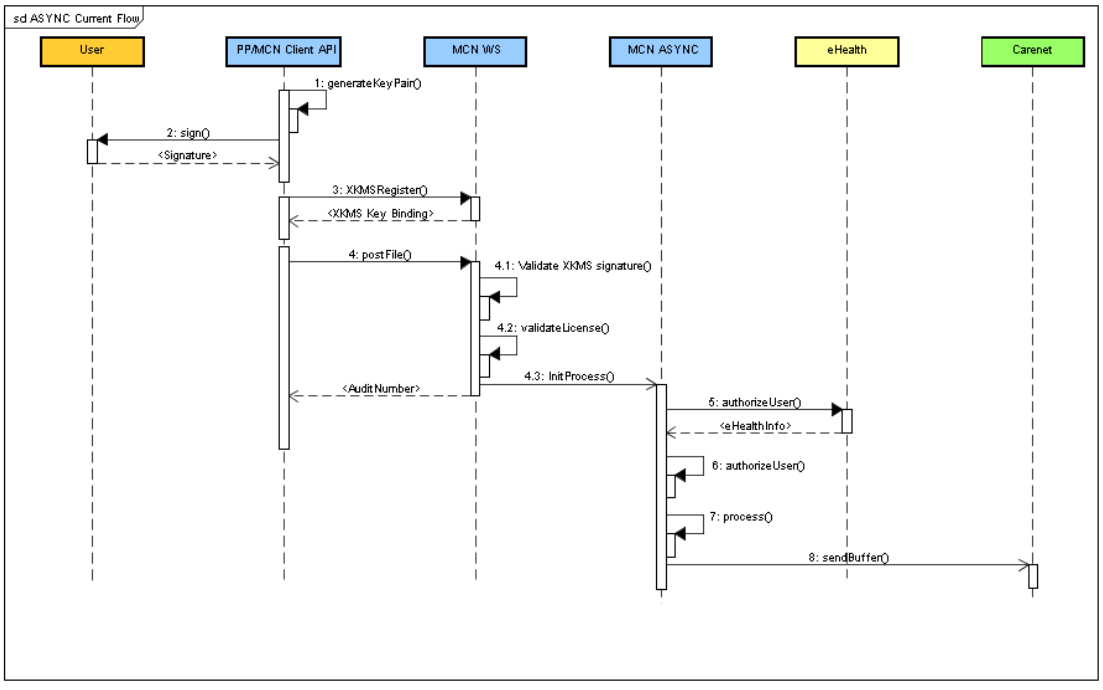
Bij de analyse van de aanvraag zal MyCareNet de identificatie informatie aan eHealth overmaken, evenals de vertaling van de rol die de gebruiker gekozen heeft.
Op basis van de raadpleging van de authentieke bronnen, zal eHealth beantwoorden door een primaire autorisatie of door een weigering.

In het geval van autorisatie levert eHealth ook bepaalde attributen bijvoorbeeld de geldigheidsduur van de mandaten. Op basis van de informatie en van de specifieke autorisatieregels van de gevraagde dienst zal MyCareNet een tweede autorisatie controle uitvoeren.

De autorisatie informatie (INSZ nummer – zorgverstrekker – rol - gevraagde dienst) wordt geplaatst in een tijdelijk geheugen van de toepassing MyCareNet. Bepaalde veiligheidsnormen beheren de geldigheidsduur van de informatie in dit tijdelijk geheugen dat als doelstelling heeft het autorisatieproces niet systematisch te moeten herhalen.

Bij volgende aanvragen detecteert MyCareNet elke eventuele wijziging aan één van de parameters die een rol spelen voor de autorisatie op. In dit geval of als de informatie van het tijdelijk geheugen vervallen is, zal MyCareNet het volledige autorisatieproces hernemen.

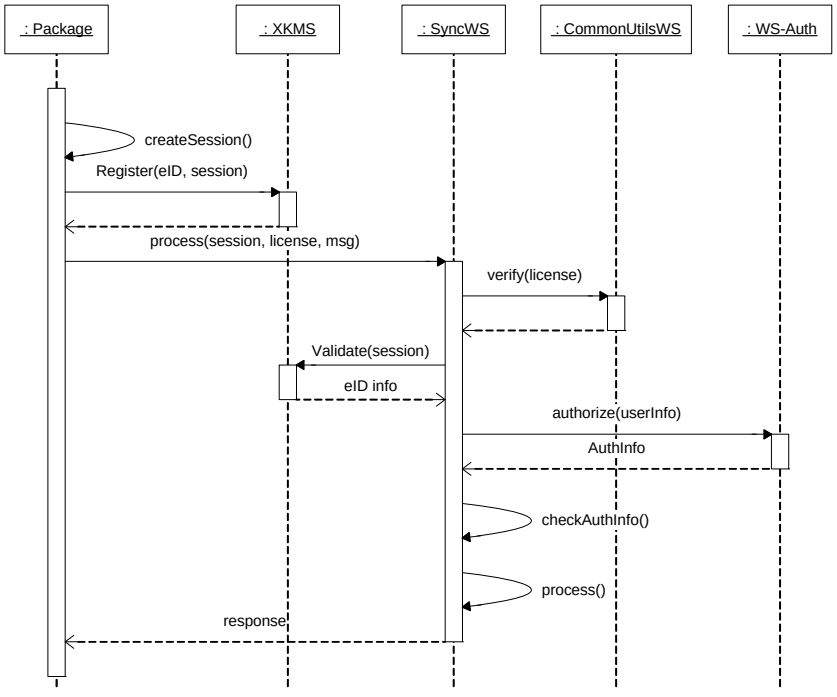
Het onderstaande schema illustreert een voorbeeld van de verschillende interacties bij een asynchrone uitwisseling :



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.

Het onderstaande schema illustreert een voorbeeld van de verschillende interacties bij een synchrone uitwisseling :



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.

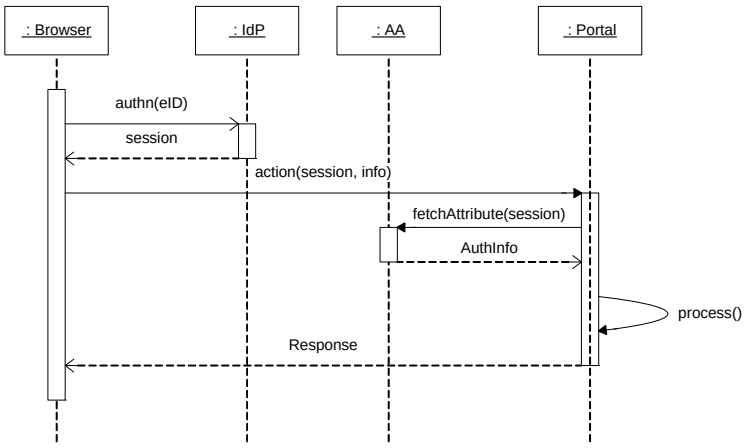
7. This extra information is checked by MyCareNet to see if the user has the right to use MyCareNet. This check consists of several sub-checks (e.g. B/W Lists)
8. The message is processed, since this does not change from the current processing, no detail is included in this document.
9. The response is returned to the package.

Bij gebruik van het portaal

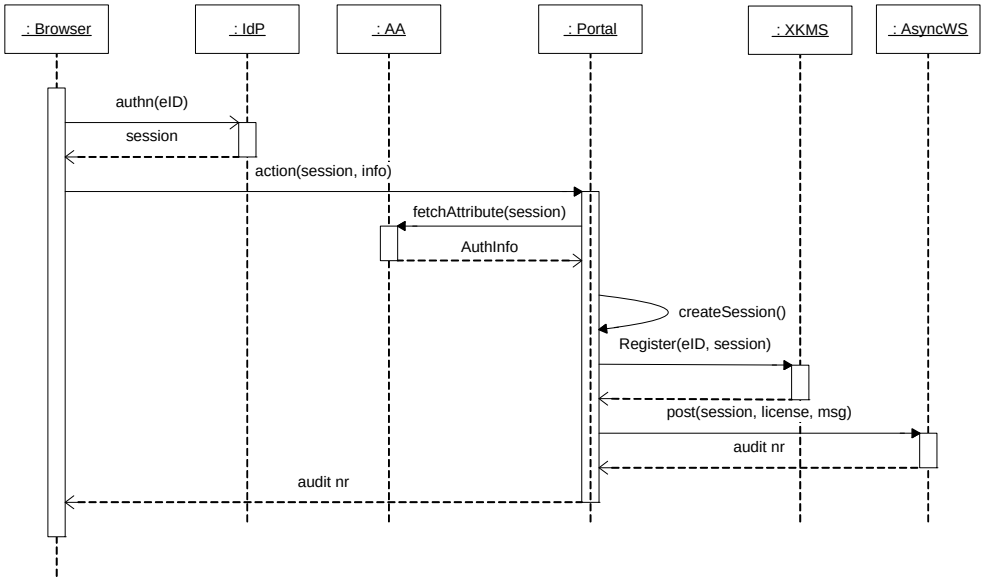
Het gebruik van het portaal is gebaseerd op gelijkaardige principes als die van de interactie systeem naar systeem maar doet beroep op andere protocollen. (Shibboleth).

Shibboleth is een middleware gebaseerd op SAML, die een authenticatie- en toestemmingsmechanisme inter-domein implementeert (Web Single SignOn) : de identity provider (IdP) levert de informatie met betrekking tot de gebruikers terwijl de Service provider (SP) deze informatie gebruikt om de toegang aan bepaalde bronnen toe te laten of niet. Zijn gebruik op het MyCareNet platform laat de authenticatie en het beheer van de gebruikers tot eHealth toe. Op basis van hun attributen zal MyCareNet nadien de toegang geven aan deze gebruikers voor bepaalde diensten.

Het onderstaande schema illustreert een voorbeeld van de verschillende interacties bij het gebruik van het portaal:



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.

Ondertekening en datering van de berichten

De facturatie bestanden en de medisch-administratieve documenten uitgewisseld binnen MyCareNet (CPD genoemd voor Care Provider Document) moeten elektronisch getekend worden voor integriteitdoelstellingen, zowel in de systeem naar systeem als in de portaal gebruiksmode.

Deze handtekening moet globaal toegepast worden op het geheel van de documenten die overgemaakt worden in een CPD.

De handtekening dient uitgevoerd te worden door middel van de standaard PKCS#7 (algoritme SHA1) op basis van een basis bestand, niet gezipt. Deze handtekening dient ingevoegd te worden als tekst in een base64 encodering in een CPD evenals het certificaat dat gebruikt wordt voor de handtekening.

De persoon die tekent kan de individuele prestatieverlener zijn of de verantwoordelijke van de groepering, alsook elke geautoriseerde MyCareNet gebruiker die door één van hen aangeduid is via het “user management” (zie de site van de sociale zekerheid) of via “mandaat” (zie de Overeenkomst MyCareNet Verpleegkundigen).

Voorwaarden met betrekking tot de informatica systemen van prestatieverleners en VI’s

Er wordt gevraagd aan de informaticasystemen van de zorgverleners en de VI’s om het volgende te voorzien :

Beschrijving van de te archiveren gegevens

Zie artikel 6 van het protocol

Beschrijving van de archiveringsprocedure

Dagelijks worden alle bestanden vermeld in “Beschrijving van de te archiveren gegevens” in twee verschillende exemplaren opgeslagen op een niet-vluchtige drager. Deze bewaarde bestanden mogen aan de eerder opgeslagen bestanden worden toegevoegd, maar moeten achteraf ervan kunnen worden losgemaakt.

Beschrijving van de procedures voor bewaring van de archieven

De archieven worden zo opgeslagen dat ze achteraf niet meer kunnen worden gewijzigd of dat elke achteraf aangebrachte wijziging op te sporen is. De archieven worden gekopieerd en bewaard op fysiek verschillende plaatsen om te voorkomen dat ze door een ongeval allemaal tegelijk zouden worden vernietigd. Deze archieven worden tegen fysieke aantastingen (brand, overstroming) beschermd en, om de vertrouwelijke aard ervan te vrijwaren, krijgen uitsluitend vooraf aangewezen personen toegang ertoe.

Beschrijving van de procedure voor opzoekingen in het archief en publicatie van de archieven

Toegang tot de gegevens kan worden verkregen door minstens onderstaande opzoekingcriteria, apart of gecombineerd, in te voeren: sender, receiver, type bericht, datum van creatie van het bestand. Wat betreft het publiceren van de archieven : zie artikel 7 van het protocol.

Beschrijving van de gebruikte informatiemiddelen, software en hardware

De gebruikte hardware, software en dragers moeten algemeen verspreid zijn en van die aard zijn dat de toepassingen even lang bewaard blijven als de maximale bewaartermijn van de gegevens. Als zou blijken dat de gebruikte techniek niet meer door de leverancier wordt aangeboden, zou de prestatieverlener of de V.I. ervoor moeten zorgen dat de informatie op een nieuwe drager wordt opgeslagen.

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.

Aansluitingsprocedure voor een software ontwikkelaar in MyCareNet

Een software pakket krijgt pas toegang tot MyCareNet nadat een geheel van administratieve stappen ondernomen zijn alsook een set van technische en business testen met het platform MyCareNet en de VI's gerealiseerd zijn.

De volledige aansluitingsprocedure voor een software ontwikkelaar is beschreven in het document « MyCareNet vademecum » dat beschikbaar is bij het Nationaal Intermutualistisch College (NIC).