MINISTÈRE
DU TRAVAIL, DE LA SANTÉ,
DES SOLIDARITÉS
ET DES FAMILLES
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Ségur du numérique en santé

Systèmes ouverts et non sélectifs (SONS)

Système d'information radiologique (RIS)

VAGUE 2

Dossier de spécifications de référencement (DSR)

DSR-IMG-RIS-Va2

Annexe II à l'arrêté relatif à un programme de financement destiné à encourager l'équipement numérique des établissements, médecins radiologues et médecins nucléaires ayant une activité d'imagerie médicale - Fonction « Système d'information de radiologie » Vague 2

Financé par
l'Union européenne
NextGenerationEU

SÉGUR
NUMÉRIQUE

LA E-SANTÉ
FRANÇAISE

Sommaire

1. PRÉSENTATION ET DÉFINITIONS 3
1.1 Présentation du dispositif SONS IMG-RIS-Va2 3
1.2 Définitions 3
2. PÉRIMÈTRE LOGICIEL ÉLIGIBLE AU RÉFÉRENCEMENT 6
3. EXIGENCES LOGICIELLES 7
3.1 Formalisme de description et règles d'application des Exigences 7
3.2 Présentation des Exigences logicielles IMG-RIS-Va2 9
3.2.1 Gestion et partage des documents de santé 9
3.2.2 Consultation et alimentation du DMP / Mon espace santé 15
3.2.3 Gestion de la MSSanté 25
3.2.4 Identification électronique & Pro Santé Connect 28
3.2.5 Sécurité des SI 32
3.2.6 Autres fonctionnalités 33
3.2.7 Conformité aux autres services socles 34
3.2.8 Identité Nationale de Santé 34
3.2.9 Exigences issues de la vague 1 RIS 40
4. MODALITES DE REFERENCEMENT DE LA SOLUTION LOGICIELLE 42
4.1. Principes de référencement de la Solution logicielle 42
4.2. Calendrier du SONS IMG-RIS-Va2 45
4.3. Phase 1 - Dépôt et validation du dossier administratif 45
4.4. Phase 2 - Dépôt de dossier complet de preuves de conformité & instruction par l'ANS 47
4.5. Phase 3 - Signature de la convention Ségur par l'Editeur et attribution du référencement 48
4.6. Espace Authentifié, Support et FAQ 49
4.7. Confidentialité 50
4.8. Protection des données à caractère personnel 50
4.9. Convention de preuve 51
5. GLOSSAIRE 52

1. PRÉSENTATION ET DÉFINITIONS

1.1 Présentation du dispositif SONS IMG-RIS-Va2

Dans le cadre du volet numérique du Ségur de la santé, l'Etat met en place des dispositifs d'achat pour compte au bénéfice des acteurs de l'offre de soins, sous la forme de systèmes ouverts et non sélectifs de référencement et de financement (SONS).

Ces dispositifs ont pour objectif d'encourager le passage à des solutions logicielles respectant certaines Exigences techniques, fonctionnelles et ergonomiques, afin de généraliser le partage fluide et sécurisé des données de santé entre professionnels de santé et avec l'usager, pour mieux prévenir, mieux soigner et mieux accompagner.

Le présent dispositif s'inscrit dans le cadre de la vague 2 du Ségur numérique, qui vise à doter d'une mise à jour logicielle conforme aux Exigences de la vague 2 le plus grand nombre possible d'acteurs de l'offre de soins, qu'ils aient ou non bénéficié de la mise à jour de la vague 1.

Le présent dispositif relatif aux logiciels de type « RIS » (Radiologic Information System) est encadré par l'arrêté du ministre chargé de la santé, consultable sur le site Légifrance, et par trois annexes qui en précisent les modalités de mise en œuvre sur les plans technique, administratif et financier :

- **Le référentiel d'Exigences et de scénarios de conformité REM-IMG-RIS-Va2**, qui définit les Exigences techniques, fonctionnelles et ergonomiques à respecter pour bénéficier du référencement, ainsi que les scénarios de vérification associés ;
- **Le dossier de spécification de référencement DSR-IMG-RIS-Va2 (présent document)**, qui présente les modalités de présentation et d'instruction des demandes de référencement ;
- **Le document d'appel à financement AF-IMG-RIS-Va2,** qui définit l'ensemble des règles et conditions associées à l'attribution et au versement des financements, ainsi que les modalités de présentation et d'instruction des demandes de financement et de paiement.

1.2 Définitions

Sauf stipulation contraire, les termes et expressions commençant par une majuscule et employés dans le présent document ont la signification qui leur est attribuée ci-après :

Chef de file : le Chef de file est désigné lorsque plusieurs personnes morales distinctes sont parties prenantes à la même demande de référencement. Le chef de file porte le composant principal de la Solution logicielle et dispose d'un mandat de la part de la ou les autres entités impliquées. Le chef de file du groupement est l'interlocuteur unique de l'ANS pendant tout le processus de référencement. Il représente le groupement pour toute démarche ou acte au titre du référencement de la Solution logicielle.

Client : le Client désigne l'Etablissement de santé, le groupe d'établissements ou structures de ville bénéficiaires de la Prestation Ségur. Le cas échéant, le Client peut renvoyer à la personne ayant le pouvoir d'engager la responsabilité de l'entité représentée.

Compatibilité ascendante : elle désigne une Solution logicielle référencée capable de respecter dans sa version N+1 plus récente, les Exigences de la version N, plus ancienne, pour laquelle elle a obtenu le référencement.

Composant principal : composant applicatif central unique, édité par le Chef de file mandataire du groupement solidaire.

Composant Proxy e-santé : composant technique sans interface utilisateur, destiné à sécuriser les échanges de données dans le cadre d'une connexion par API Pro Santé Connectée, et ayant vocation à être habilité au sein de l'Espace de confiance PSC, selon les modalités du référentiel Pro Santé Connect.

Composant additionnel : composant applicatif édité par un membre du groupement solidaire ou un Editeur tiers, hors mandataire. On entend par Composants additionnels intégrés un ensemble de composants interagissant entre eux sans que l'utilisateur n'ait à faire d'opérations spécifiques.

Convergence : la plateforme Convergence désigne le portail de service en ligne géré par l'ANS permettant le référencement d'une Solution logicielle (dépôt du dossier administratif, dépôts des preuves et instructions des preuves de conformités aux exigences, attribution du référencement).

Distributeur : toute personne physique ou morale, publique ou privée, ou tout groupement de personnes, doté ou non de la personnalité morale, qui distribue la Solution logicielle référencée, c'est à dire qui le commercialise auprès de l'établissement ou du professionnel de santé et porte le contrat d'utilisation de la Solution logicielle avec le client final, dans la seule hypothèse où ce distributeur est mandaté par l'Editeur pour déposer une demande de financement auprès de l'opérateur de paiement.

Editeur : toute personne physique ou morale, publique ou privée, ou tout groupement de personnes, doté ou non de la personnalité morale, qui édite la Solution logicielle, candidate au référencement par l'Agence du Numérique en Santé.

Espace Authentifié : espace sécurisé du Portail Industriels (https://industriels.esante.gouv.fr) permettant à l'Editeur d'accéder à des services spécifiques et à des informations personnalisées et adaptées à ses besoins.

Exigences : spécifications (générales, techniques ou détaillées) présentées dans le référentiel d'Exigences et de scénarios de conformité REM-IMG-RIS-Va2.

Groupement solidaire : lorsque plusieurs personnes morales distinctes sont parties prenantes à la même demande de référencement, elles constituent un groupement représenté devant l'ANS par un Editeur Chef de file et sont solidairement responsables au regard des obligations visées dans le présent document.

ISC : le fournisseur d'identité Industriels Santé Connect (iSC) repose sur un répertoire d'identité unique des entreprises associé à une politique d'identification électronique de leurs collaborateurs, partagée avec les applications qui lui sont rattachées ou fournisseurs de service. iSC offre à ses utilisateurs une fonctionnalité de *Single-Sign On (SSO),* leur permettant de se connecter à ces applications ou fournisseurs de services dont la plateforme Convergence et l'Espace Authentifié du Portail Industriels, sans avoir à se réauthentifier, avec un moyen d'identification électronique à double facteur d'authentification, *Time based One Time Password (TOTP)* par courriel.

KOS (ou Manifest KOS) ME : est un document normalisé par le standard DICOM, contenant un pointeur référençant un examen d'imagerie médicale d'un patient. Le KOS référence l'ensemble des identifiants que comporte un examen d'imagerie.

Périmètre vague 1 ou vague 2 : le Périmètre vague 1 et le Périmètre vague 2 renvoient à l'onglet « Exigences » du REM-IMG-RIS-Va2. Le Périmètre vague 1 renvoie aux exigences conservées de la vague 1, et le Périmètre vague 2 renvoie aux nouvelles exigences de la vague 2.

Prestation Ségur : la Prestation Ségur désigne l'une des deux Prestations Ségur vague 2 (Prestation Ségur vague 2 et Prestation vague 1 + vague 2) dont les périmètres sont décrits à la Section 3 de l'AF-IMG-RIS-Va2.

Profil : un Profil est un regroupement d'Exigences. Le Profil général regroupe les Exigences applicables à toutes les Versions candidates au référencement. Les autres Profils regroupent des Exigences conditionnelles, qui ne sont applicables que si l'Editeur choisit de candidater pour ce(s) Profil(s).

Solution logicielle : une solution logicielle est constituée d'un Composant principal, d'un Composant Proxy e-santé, et éventuellement complété d'un ou plusieurs Composants additionnels intégrés dans une version majeure identifiée et référencée par l'ANS. Au sein du présent document, sauf mention spécifique, le terme

Solution logicielle désigne donc l'ensemble constitué du Composant principal, du Composant Proxy e-santé, et du ou des éventuels Composants additionnels.

Version candidate : version d'une Solution logicielle éligible soumise par un Editeur à l'ANS pour devenir la version référencée et identifiée par un Numéro de version technique unique. Le référencement est délivré pour une Version candidate d'une Solution logicielle. Le référencement précise le ou les Profils pour lesquels la Solution Candidate a satisfait aux Exigences.

2. PÉRIMÈTRE LOGICIEL ÉLIGIBLE AU RÉFÉRENCEMENT

Le référencement IMG-RIS-Va2 concerne la fonction « RIS » (Radiologic Information System) des établissements de santé, qui a vocation à gérer les rendez-vous patients, programmer les modalités d'imagerie, générer et envoyer les comptes-rendus de radiologie.

Une Solution logicielle souhaitant candidater au référencement en tant que RIS doit comporter, a minima, les fonctions suivantes :

- Gestion des rendez-vous patients ;
- Programmation des examens d'imagerie avec génération de l'identifiant Study Instance UID ;
- Génération et envoi des comptes-rendus radiologiques ;
- Un RIS met à disposition une liste de travail « DICOM Modality Worklist » et produit au minimum des messages HL7 de type ADT, ORU et ORM ;
- Fonctionnalités permettant le fonctionnement de la DRIMbox et son appel depuis le RIS.

Les domaines concernés par ce DSR sont :

- La Radiologie conventionnelle ;
- La Mammographie ;
- Le Scanner ;
- L'Imagerie par Résonnance Magnétique (IRM) ;
- La Médecine Nucléaire ;
- L'échographie.

Ne sont pas éligibles au référencement les logiciels suivants :

- Logiciels de Cardiologie ;
- Logiciels d'Imagerie dentaire ;
- Logiciels de Génétique ;
- Lecteurs de documents marqués ;
- Middleware (connexion d'automates, microbiologie sans papier) ;
- Catalogues d'examens ;
- Systèmes experts d'aide à la décision ;
- Logiciels de prescription connectée ;
- Serveurs de résultats ;
- Logiciels de gestion documentaire et de qualité ;
- Logiciels de gestion des stocks ;
- Solution permettant un archivage et une diffusion des images : PACS ;
- Serveur d'Archives Neutres : VNA.

3. EXIGENCES LOGICIELLES

3.1 Formalisme de description et règles d'application des Exigences

Formalisme de description des Exigences

Les Exigences à respecter sont décrites dans le référentiel d'Exigences et de scénarios de conformité **REM-IMG-RIS-Va2.**

A chaque Exigence est associée une modalité de vérification, qui sera mise en œuvre dans le cadre du référencement. Certaines Exigences concernent la conformité à certains référentiels, dans leur version précisée dans le REM.

Au-delà des Exigences dont la conformité est vérifiée dans le cadre du référencement, l'Editeur doit se conformer à l'ensemble du cadre réglementaire applicable à son activité et à la Solution logicielle qu'il met en œuvre. Les référentiels d'interopérabilité et de sécurité élaborés par l'ANS lui sont opposables dans les conditions définies aux art. L. 1470-5 et s. du code de la santé publique.

Profils applicables à la solution candidate au référencement

Dans le REM, le Profil « Général » regroupe les Exigences applicables à toutes les Versions candidates au référencement.

Les autres Profils regroupent des Exigences qui ne s'appliquent qu'aux Editeurs ayant choisi de faire référencer leur Solution logicielle comme étant conforme à ces Exigences au vu des conditions associées à chaque Profil, et précisées ci-dessous.

Dans le cadre de la procédure de référencement, détaillée à la Section 4 du présent document :

- L'Editeur identifie le(s) Profil(s) qui s'applique(nt) à sa solution ou qu'il choisit de solliciter pour la solution qu'il présente au référencement ;
- L'ANS référence la Solution logicielle, en tenant compte des Exigences associées au(x) Profil(s) choisi(s) par l'Editeur ;
- L'attestation finale de référencement remise à l'Editeur indique le(s) Profil(s) pour le(s)quel(s) la solution a été référencée.

Pour le REM-IMG-RIS-Va2, les Profils disponibles et les critères de choix sont définis dans le tableau ci-dessous :

Profil	Critère(s) de choix des Profils *(Profil à sélectionner par l'Editeur dans les cas suivants)*
Général	N/A (Profil imposé à toutes les solutions candidates au référencement)
Gestion double authentification avec SMS / email	Obligatoire dès lors que l'Editeur a choisi d'implémenter dans sa solution un mécanisme de vérification des identités des professionnels via sms ou email
CIBA	Obligatoire dès lors que l'Editeur a choisi d'implémenter dans sa solution l'authentification PSC par CIBA

Cas des solutions déjà référencées en vague 1

Dans le REM-IMG-RIS-Va2, chaque Exigence relève :

- Soit du Périmètre vague 2, qui rassemble les Exigences élaborées à l'occasion du présent dispositif ;
- Soit du Périmètre vague 1, qui rassemble les Exigences déjà présentes dans le dispositif publié à l'occasion de la vague 1 du Ségur numérique.

A noter : *le Périmètre vague 1 a été révisé par rapport aux dispositifs publiés dans le cadre de la vague 1 :*

- Certaines Exigences de la vague 1 ne sont pas reprises, car rendues « obsolètes » par des Exigences du Périmètre vague 2 couvrant les mêmes fonctionnalités ;
- Les Exigences de la vague 1 qui relevaient de l'un des Profils optionnels suivants sont désormais intégrées au profil Général de la vague 2 et donc imposées à toute Solution candidate :
    - Authentification électronique unipersonnel avec utilisation du RPPS-Rang pour les cabinets libéraux en SCM (Société Civile de Moyen) ;
    - Envoi manuel par MSS au PS Demandeur ;
    - Référentiel d'identités.

Pour le REM-IMG-RIS-Va2, les règles sont les suivantes :

- Si la solution candidate a été référencée au titre du dispositif IMG-RAD-Va1 et l'Editeur est titulaire d'une attestation de référencement au titre du dispositif IMG-RAD-Va1, avec les trois profils suivants :
    - Authentification électronique unipersonnel avec utilisation du RPPS-Rang pour les cabinets libéraux en SCM (Société Civile de Moyen) ;
    - Envoi manuel par MSS au PS Demandeur ;
    - Référentiel d'identités.

  Alors, l'Editeur est dispensé du dépôt des preuves des Exigences du Périmètre vague 1. Ainsi, les preuves déjà fournies et vérifiées lors du référencement d'un couple solution / éditeur en vague 1 seront considérées comme valides dans le cadre du référencement de ce même couple solution / éditeur en vague 2.
- Si la solution candidate a été référencée au titre du dispositif IMG-RAD-Va1 et l'Editeur est titulaire d'une attestation de référencement, sans au moins l'un des profils suivants :
    - Authentification électronique unipersonnel avec utilisation du RPPS-Rang pour les cabinets libéraux en SCM (Société Civile de Moyen) ;
    - Envoi manuel par MSS au PS Demandeur ;
    - Référentiel d'identités.

  Alors, seul le dépôt des preuves du Périmètre vague 1 correspondant aux exigences du ou des Profil (s) manquant(s) lors du référencement en vague 1 est exigé.

Bien qu'un dépôt de toutes les preuves du Périmètre vague 1 ne soit pas exigé, le couple solution / éditeur en vague 2 doit respecter le périmètre de ces exigences.

Par exception à ce qui précède, l'ANS se réserve le droit d'exiger le dépôt de certaines preuves relevant d'Exigences du Périmètre vague 1, en particulier en cas de manquement constaté de l'Editeur aux obligations couvertes par la convention de référencement signé avec l'ANS dans le cadre de la vague 1.

3.2 Présentation des Exigences logicielles IMG-RIS-Va2

Les exigences et scénarios de conformités présentés dans le document **REM-IMG-RIS-Va2** couvrent les chapitres suivants :

1. **Gestion et partage des documents de santé**
2. **Consultation et alimentation du DMP / Mon espace santé**
3. **Gestion de la MSSanté**
4. **Identification électronique & Pro Santé Connect**
5. **Sécurité des SI**
6. **Autres fonctionnalités**
7. **Conformité aux autres services socles**
8. **Identité Nationale de Santé**
9. **Exigences issues de la vague 1 RIS (périmètre « Vague 1 »)**

3.2.1 Gestion et partage des documents de santé

Objectifs pour le RIS en vague 2 :

Le Ségur du numérique en santé définit des exigences permettant aux professionnels de santé de disposer de logiciels à même de **produire et partager les documents de santé dans des formats enrichis et interopérables**, en particulier sur les objectifs suivants :

- Permettre la **visualisation des documents de santé** consultés dans le DMP ou reçus par MSSanté au format CDA en particulier pour l'affichage des métadonnées des documents ou dans le cas des documents au format CDA R2 N3 avec un PDF encapsulé (en première intention visualisation du PDF et si l'utilisateur le demande afficher le document CDA R2 N3 avec une feuille de style).
- Permettre à l'utilisateur depuis le dossier du patient en local d'exploiter au mieux les documents disponibles dans le DMP ou reçus par MSSanté :
    - Informer l'utilisateur qu'un document du DMP est déjà présent dans le dossier du patient en local ;
    - Informer l'utilisateur qui consulte un document dans le dossier local qu'une version plus récente du document est disponible dans le DMP du patient ou que le document a été supprimé ;
    - Identifier parmi tous les documents du logiciel **les documents importés depuis le DMP et la MSSanté,** afin que l'utilisateur soit conscient de sa provenance sans clic notamment en cas de problème ;
    - Trier les documents importés et produits pour accéder facilement au document recherché.
- Permettre à l'utilisateur depuis le dossier du patient en local de partager au mieux les documents disponibles dans le DMP ou reçus par MSSanté :
    - Identifier parmi tous les documents du logiciel les documents envoyés vers le DMP et la MSSanté, afin que l'utilisateur puisse envoyer ceux qui ne l'ont pas encore été (dans un but de partage des documents présents historiquement dans le logiciel) ;
    - Produire un document avec un contenu cohérent quel que soit son format (PDF/A-1, CDA R2 N1, CDA R2 N3).

La vague 2 vient également imposer la **standardisation des flux d'interopérabilité entre les fonctions RIS et la PFI :**

- Implémenter le volet du CI-SIS ***Transmission de document(s) CDA en HL7v2***, afin que le RIS puisse transmettre les documents qu'il produit à destination de la fonction PFI chargée d'alimenter le DMP et/ou d'envoyer le(s) document(s) en pièce jointe d'un courrier électronique MSSanté à des destinataires.

- Implémenter le volet du CI-SIS ***Transmission au LPS de documents CDA provenant d'un courriel MSSanté*** afin que le RIS puisse intégrer des courriels MSSanté reçus sur des BAL applicatives et exploitées par la fonction PFI d'un établissement de santé.

Fonctionnalités couvertes par les exigences vague 2 :

N°	GESTION ET PARTAGE DES DOCUMENTS DE SANTE - Fonctionnalités du périmètre Vague 2	Exigences associées
1.1	**Affichage des documents au format CDA R2 N1 et N3**	
	Mise en visibilité de la copie PDF encapsulée qui doit affichée de préférence lors de l'ouverture pour les documents CDA R2 N3. Possibilité de basculer vers le format CDA R2 N3 via la feuille de style de l'ANS ou du producteur Affichage des métadonnées des documents CDA R2 N3 et PDF associés sur une seule ligne dans l'espace documentaire	SC.CDA/DD.15 SC.CDA/VISU.03 SC.CDA/VISU.01
1.2	**Production des documents au format CDA R2 conformes au CI-SIS**	
	Pré-remplissage des documents avec les informations présentes dans le dossier du patient Production des documents au format CDA intégrant le Datamatrix et marquage 'INS à scanner'	SC.DOC.03 SC.CDA/VISU.04
1.3	**Navigation dans le dossier patient local et identification des documents importés depuis / exporté vers le DMP et la MSSanté**	
	Identification (sans clic) dans le dossier patient des documents importés depuis le DMP et la MSSanté Identification dans le dossier patient des documents exportés vers le DMP et la MSSanté Affichage (sans clic) du statut de l'identité du patient (provisoire, validée, récupérée, qualifiée), au niveau de l'interface "dossier patient" Tri des documents importés et produits, à minima, selon le type code et la date de l'acte Absence de blocage de l'interface graphique de l'utilisateur pendant les requêtes au DMP, Pro Sante Connect et l'Annuaire	SC.CDA/INT.04 SC.CDA/INT.08 SC.CDA/INT.17 SC.DMP/HISTO.01 DPI.DMP/UX.10 SC.DMP/UX.11
1.4	**Information de l'existence et visualisation d'une version plus récente d'un document déjà intégré dans le dossier patient**	
	Notification de l'utilisateur lors de la consultation d'un document au sein du dossier d'un patient si une version plus récente de ce même document est disponible dans le DMP. Accès direct à la dernière version du document et intégration dans son RIS	SC.CDA/DD.05 SC.CDA/VISU.02
1.5	**Gestion des documents CDA**	
	-Intégration / remplacement et suppression d'un document CDA suite à réception d'un document CDA par messagerie sécurisée de santé	SC.CDA/INT.18
1.6	**Interopérabilité entre le RIS et la fonction PFI en environnement hospitalier**	
	- Mise en œuvre des volets d'interopérabilité entre les fonctions RIS et PFI pour la gestion des documents CDA envoyés (DMP, MSSanté) et reçus (MSSanté) - Gestion des acquittements techniques et métiers de réception d'un document via la fonction PFI - Transmission à la fonction PFI via le flux HL7 V2 les informations d'identification nécessaires à la constitution du jeton VIHF	SC.CDA/HL7.01 SC.CDA/HL7.02 SC.CDA/HL7.04 SC.DMP/CONF.12
1.7	**Gestion des demandes et CR d'imagerie médicale - DRIMbox**	
	- Création d'une demande RIS en regard des demandes d'acte d'imagerie - Intégration des métadonnées spécifiques à l'imagerie sur un CR d'imagerie - Ajout des lien URL et QR d'accès aux images des examens correspondants - Echange des données avec la DRIMbox source via des messages HL7 de type ORU ou MDM - Appels contextuels vers la DRIMBox conso avec gestion du consentement du patient	SC.DB/RIS.04 SC.DB/RIS.09 SC.DB/RIS.11 SC.DB/RIS.12 SC.DB/TRA.05
1.8	**Eviction des conflits entre documents identiques**	
	Génération d'un document au format CDA, PDF/A-1 à partir des mêmes données	SC.CDA/DD.24
1.9	**Téléradiologie et télémédecine nucléaire**	
	-Réception d'un document CDA sur la base d'un message HL7 V2 ORU provenant des plateformes de téléradiologie. - Alimentation du DMP à la suite d'une demande ORU d'intégration, de modification ou de suppression d'un compte rendu par une plateforme de téléradiologie, avec possibilité de déclencher l'action suivant un délai paramétrable	RIS.TLR/INT.01 RIS.TLR/INT.02

Affichage des documents au format CDA R2 N1 et N3

En vague 1, le choix avait été fait de produire 2 comptes-rendus d'examen de biologie médicale distincts : un document au format CDA R2 N1 incluant le compte rendu au format PDF et un document au format CDA R2 N3 au format structuré.

Cette solution présente plusieurs inconvénients en termes d'espace de stockage de documents, de lisibilité de l'espace documentaire des logiciels de professionnels de santé ou de Mon espace santé (doublonnage des documents notamment) et risque d'erreur de masquage ou d'invisibilisation des documents (masquage uniquement du document CDA R2 N1 et pas du document CDA R2 N3, par exemple).

En vague 2, les documents structurés seront produits uniquement au format CDA R2 N3 avec une section spécifique portant le PDF dans le corps structuré du document CDA pour les documents au format CDA R2 N3 suivants générés par les autres logiciels : compte-rendu d'examen de biologie médicale, par exemple (voir Volet de référence Modèles de contenus CDA). Le RIS va consommer ces documents et doit avoir la capacité de les afficher correctement en affichant de préférence le PDF.

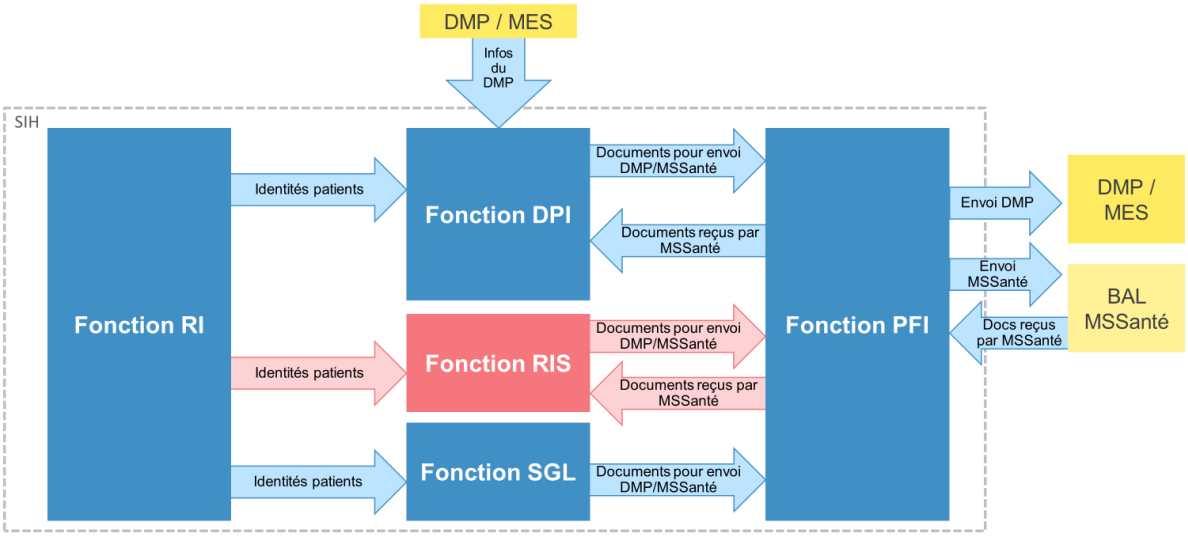
Interopérabilité des fonctions RIS et PFI en environnement hospitalier

Transmission de documents CDA en HL7v2 : il s'agit d'une transaction de demande de transmission/remplacement/suppression de document(s) clinique(s) entre un système créateur de documents et une fonction PFI, dans l'objectif de partager et/ou d'échanger ces documents avec les acteurs externes à l'établissement pour la publication de document(s) clinique(s) du patient au DMP, et l'envoi à différents destinataires externes à l'établissement au moyen de la MSSanté.

Transmission au LPS d'un document CDA provenant d'un courriel MSSanté (nouveau pour la vague 2) : il s'agit d'une transaction de demande de traitement concernant un document clinique au format CDA-R2 (demande d'intégration/de remplacement/de suppression d'un document) entre la fonction PFI de l'établissement et le logiciel métier destinataire après détection par la fonction PFI d'un courriel dans une Boîte Aux Lettres (BAL) applicative MSSanté de l'établissement.

Ces deux volets comprennent des champs permettant notamment d'indiquer si le document a été mis à jour ou supprimé dans le système producteur de document, ainsi que de transmettre et récupérer les accusés de réception DMP et MSSanté.

Par ailleurs, la conformité à ces deux référentiels permet de gérer la transmission au DMP de CR d'imagerie produit par un système tiers, par exemple en téléradiologie.



Flux d'interopérabilité avec la fonction RIS dans un contexte avec PFI

Rappel réglementaire : obligations de partage par voie numérique des documents de santé

La gestion des documents de santé doit in fine permettre le partage des documents de santé, conformément aux obligations présentes dans l'article L. 1111-15 du Code de la santé publique. Cet article

décrit les **obligations de partage par voie numérique** des « *éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge* » pour les professionnels de santé.

Ce partage s'effectue à deux niveaux :

- A travers l'alimentation du DMP / Mon espace santé
- Par envoi via messagerie sécurisée au médecin traitant, au médecin prescripteur s'il y a lieu, à tout professionnel dont l'intervention dans la prise en charge du patient lui paraît pertinente ainsi qu'au patient.

Depuis sa rédaction issue de la loi « ASAP » du 7 décembre 2020, la liste des documents sur lesquels porte cette obligation est fixée par arrêté de la ministre chargée de la santé et de l'accès aux soins, en tenant compte du déploiement des mises à jour logicielles permettant de systématiser ces partages numériques, avec la possibilité laissée au professionnel de retenir un envoi lorsque souhaité.

Identité Nationale de Santé (INS)

Pour rappel, tous les documents de santé doivent depuis janvier 2021 être référencés avec une INS.

Pour rappel, il est important de dissocier les deux types de flux d'alimentation : envoi au Dossier Médical Partagé (DMP) et envoi via la messagerie sécurisée de santé (MSSanté).

Ces 2 canaux répondent à des prérequis différents quant à la qualification de l'INS :

- La qualification de l'INS est obligatoire au versement dans le DMP / Mon espace santé
- La qualification de l'INS n'est pas obligatoire pour l'envoi des documents via la MSSanté

Bien qu'il soit fortement recommandé de transmettre des documents avec une INS qualifiée, il est possible de transmettre par MSSanté des documents sans INS qualifiée aux professionnels de santé, afin de sécuriser la transmission des informations nécessaires au suivi de son patient.

De même, pour qu'un professionnel puisse écrire à un patient (<MatriculeINS>@patient.mssante.fr), son INS doit en principe être qualifiée. Toutefois, une dérogation est intégrée dans le Référentiel #2 Client de Messagerie pour prendre en compte les cas d'usage de la préadmission et la réalité de la qualification de l'INS, cette dérogation restera valable jusqu'à révocation dans une future version du même référentiel.

Gestion des demandes et CR d'imagerie médicale - DRIMbox

À la suite de la transmission du compte-rendu d'imagerie médicale au DMP et après avoir réceptionné l'acquittement positif en réponse, le RIS devra envoyer le compte-rendu à la DRIMbox associée à travers un connecteur HL7 de transport spécifié par le volet de Transmission de document(s) CDA en HL7v2.

Pour permettre le partage des examens d'imagerie par la DRIMbox, le compte-rendu devra contenir :

- Les identifiants liés aux examens d'imageries et demandes RIS ;
- Les métadonnées descriptives des images (Modalité d'examen et région anatomique) ;
- L'URL et le QR code donnant accès aux images via la visionneuse de la DRIMbox ainsi que la durée de mise à disposition.

Ces données, en complément de celles contenues dans le message HL7 et de celles récupérées dans le PACS, permettront la construction d'un pointeur de Références d'objets d'un Examen d'Imagerie (manifest KOS) qui sera aussi envoyé au DMP.

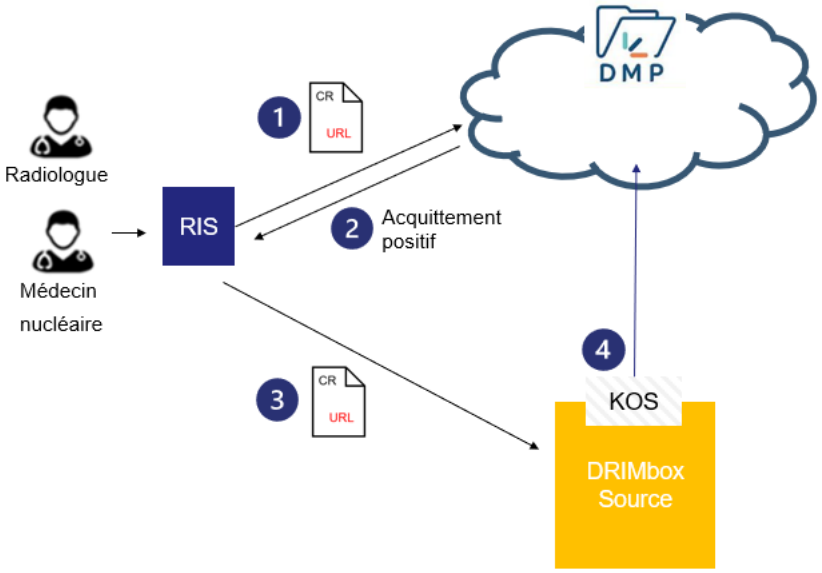


Schéma du lien entre RIS et DRIMbox source

Le RIS est ensuite maître des modifications et suppressions du compte-rendu et doit transmettre ces éléments au DMP ainsi qu'à la DRIMbox à travers un connecteur HL7 de transport spécifié par le volet de Transmission de document(s) CDA en HL7v2.

Pour avoir accès aux images partagées, le RIS doit être en mesure de faire des appels contextuels à la (aux) DRIMbox locale(s) consommatrice(s) en récupérant et en intégrant en amont l'information du consentement du patient.

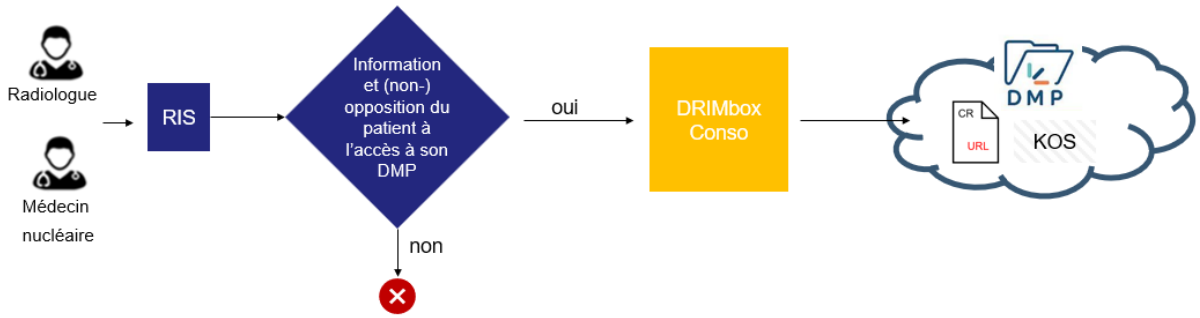
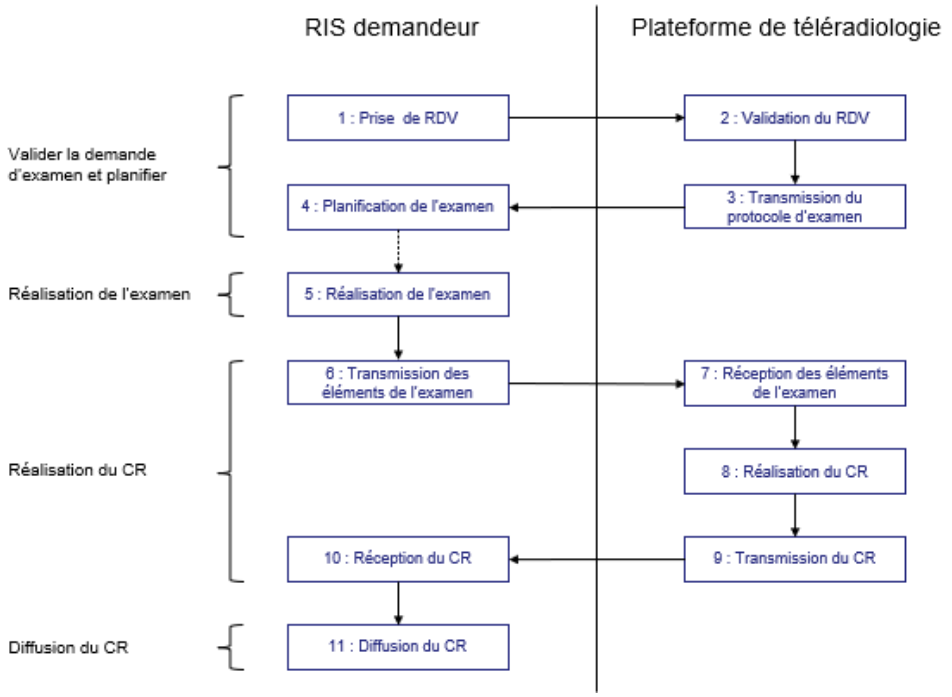


Schéma du lien entre RIS et DRIMbox conso

Téléradiologie et télémédecine nucléaire

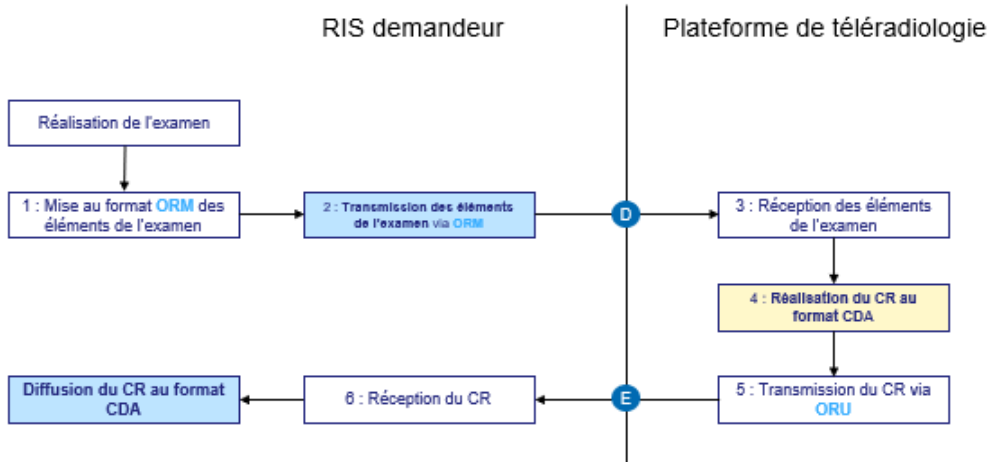
Le RIS doit transmettre dans tous les cas le compte-rendu au DMP, qu'il soit produit directement par le RIS ou en amont par un autre système qui le transmet au RIS (PACS, plateforme de téléradiologie, télémédecine nucléaire). Dans cette configuration le RIS joue en quelque sorte le rôle d'une PFI et ne doit pas modifier le contenu du CR qui a été produit à distance pas un médecin n'appartenant pas à l'organisation.

Le principe général du workflow est le suivant :



Les flux à mettre en place pour la bonne transmission des demandes et la bonne réception du CR sont les suivants.

- Flux “aller” d’envoi des demandes d’examens au format ORM avec INS
- Flux “retour” de la plateforme au format ORU intégrant les comptes rendus au format CDA R2 N1, en vue de leur intégration dans le RIS et de leur envoi dans le DMP



La mise en œuvre de cette exigence est basée sur les volets du CI_SIS publiés par l’ANS suivants :

- Le volet de Structuration minimale des documents de santé ➔ format CDA format CDA
- Le corpus documentaire du projet DRIM-M
- Le volet Transmission de document(s) CDA en HL7v2 ➔ format ORU format ORU

Le standard HL7v2 n’est plus mis à jour depuis la version HL7 v2.3.1 pour le message ORM.

Il est recommandé également la prise de connaissance des documents suivant :

- Le volet Partage de documents de santé
- Le volet Echange de documents de santé
- Le volet IMG CR d’imagerie
- Le volet IMG Demande d’actes d’imagerie

3.2.2 Consultation et alimentation du DMP / Mon espace santé

La consultation et l'alimentation du DMP du patient constitue le cœur du Ségur numérique, avec :

a) Les enjeux d'enregistrement de **l'information et des consentements du patient** ;
b) La consultation, directement depuis le logiciel métier, du DMP du patient par un membre de l'équipe de soins qui le prend en charge, et qui constitue l'objectif majeur de la vague 2 du Ségur numérique ;
c) L'alimentation systématique du DMP du patient avec les copies numériques des documents qui lui sont remis à chaque épisode de prise en charge, en renforçant les fonctionnalités déjà présentes en vague 1 ;
d) Enfin, **l'amélioration de la gestion de la visibilité des documents de santé pour les patients**, en particulier dans le cadre des consultations d'annonce effectuées par les professionnels de santé.

a) Information et consentement du patient

Objectifs pour le RIS en vague 2 :

L'objectif de la vague 2 est de garantir **l'information du patient** concernant l'alimentation et la consultation de son profil Mon espace santé, et il doit pouvoir **exprimer son opposition à l'alimentation** et **son consentement à la consultation** et conditionner ainsi le comportement du logiciel.

- Le patient doit être informé de l'accès (alimentation et consultation) à son profil Mon espace santé.
- L'**alimentation du DMP /Mon espace santé peut se faire par défaut**, cependant le patient peut s'y opposer sur motif légitime. Le motif légitime n'est pas enregistré ni véhiculé dans les Logiciels. Le professionnel peut changer le choix au cours de la prise en charge.
- La **consultation du DMP /Mon espace santé ne peut se faire que sur consentement explicite** du patient, celui-ci n'a pas à justifier son refus.
- Ces autorisations peuvent être renseignées à l'initiation de la prise en charge et doivent être **accessibles et modifiables** ultérieurement par le professionnel, par exemple en cliquant sur le bouton évoqué dans l'exigence SC.DMP/UX.13. Le patient doit pouvoir changer d'avis à tout moment de la prise en charge.
- Lorsque c'est possible, cette information et le recueil des autorisations du patient sont réalisées **en amont de la prise en charge** du patient par un professionnel, ou informatiquement par le patient lui-même (lors d'une prise rendez-vous, à l'admission ou à l'accueil, lors de l'examen).
- Dans les situations d'urgence uniquement où le patient n'est pas en état de donner son consentement, un accès en mode "**bris de glace"** est possible. Cette possibilité d'accès peut être mise en évidence pour les professionnels de santé dans le cadre de la prise en charge, mais n'est pas pertinente en amont des soins ou pour des non professionnels de santé.
- L'information et le consentement du patient sont enregistrés et s'appliquent à l'ensemble de l'**équipe de soin** prenant en charge le patient pendant la durée de l'**épisode de soin,** et non à la maille individuelle du professionnel.
- L'épisode de soin correspond à la période de prise en charge du patient. Si l'épisode de soin se poursuit après l'expiration de la durée d'autorisation technique à la consultation du DMP /Mon espace santé (ex : prise en charge au long court), la transaction d'autorisation sera renouvelée automatiquement après cette durée, sans redemander aux professionnels de recueillir à nouveau et/ou retracer le consentement.

Fonctionnalités couvertes par les exigences vague 2 :

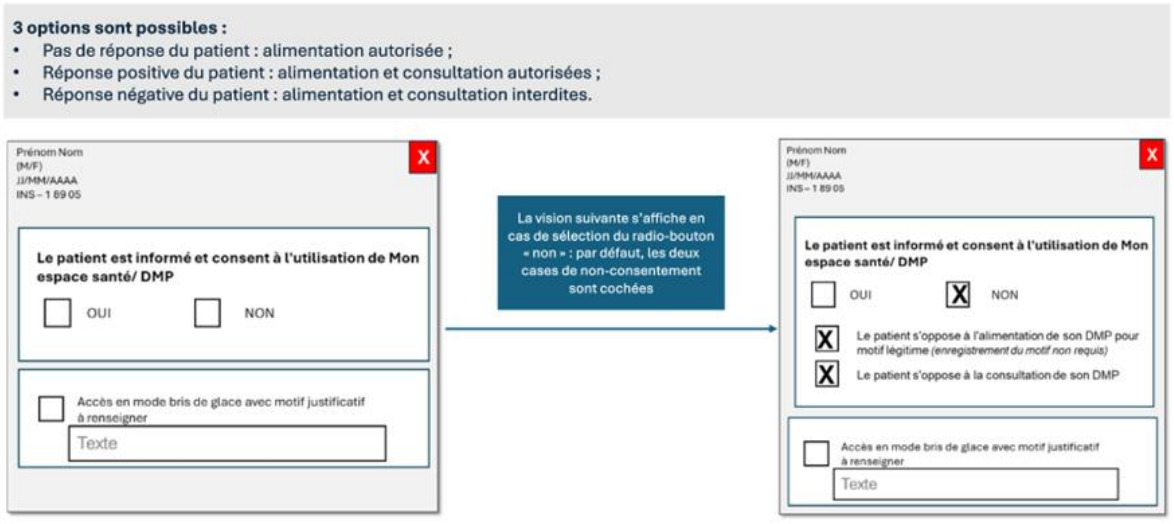
	Information et non opposition du patient à l'alimentation et consentement à la consultation du DMP / Mon espace santé - Fonctionnalités périmètre Vague 2	Exigences associées
2.1	**Gestion de l'information et du consentement du patient**	
	- Enregistrement et traçage de l'information du patient et son consentement à la consultation du DMP, la non-opposition par défaut ou l'opposition du patient à l'alimentation du DMP et respect des droits d'accès qui en résulte, pour chaque épisode de soin - Interopérabilité pour l'information et consentement à la consultation et la non-opposition à l'alimentation du patient avec le reste du SIH via le flux IHE PAM	SC.DMP/CONF.06 SC.DMP/CONF.06.BIS SC.DMP/CONF.09.BIS SC.DMP/CONF.13

Logique de comportement des logiciels en fonction de la réponse du patient :

- Pour l'alimentation du DMP / MES :
  - Valeur par défaut : le professionnel / établissement peut alimenter le DMP / MES
  - Patient informé et non opposé : il peut alimenter le DMP / MES
  - Patient informé et opposé : il ne peut pas alimenter le DMP / MES
- Pour la consultation du DMP / MES :
  - Valeur par défaut : le professionnel / établissement ne peut pas consulter le DMP / MES
  - Patient informé et consent : il peut consulter le DMP / MES
  - Patient informé et ne consent pas : il ne peut pas consulter le DMP / MES

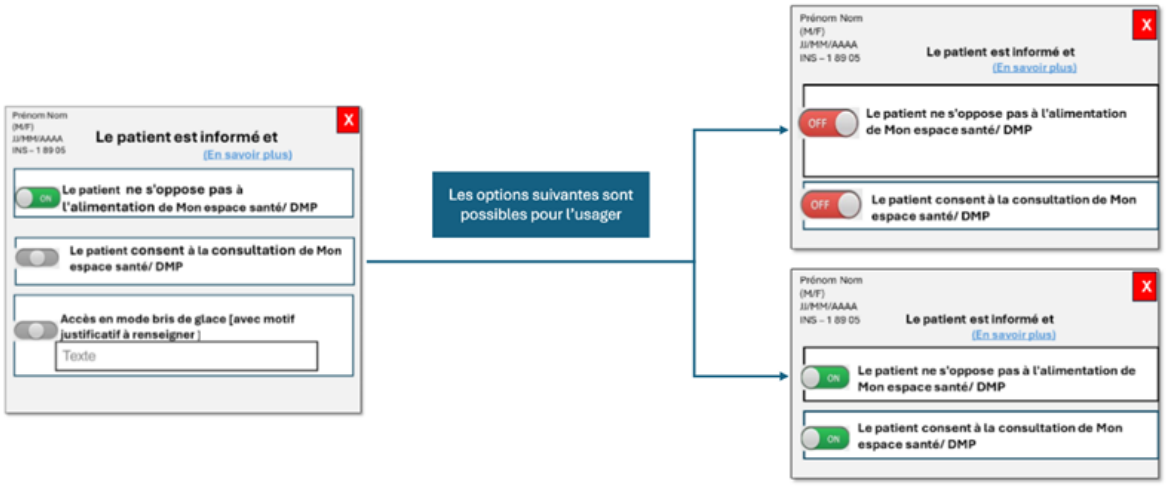
Exemples d'interfaces de traçabilité de l'information et du recueil de la non-opposition à l'alimentation du DMP et de consentement à la consultation du DMP dans le logiciel métier, en 1 clic

1er exemple :



2ème exemple :

Sans action par défaut, seul le bouton de non-opposition à l'alimentation est coché :
- L'alimentation est **possible**
- La consultation **n'est pas possible.**
- La coche d'un bouton sur la consultation est **obligatoire**



Mise à jour du flux IHE PAM pour véhiculer l'information et opposition/non-opposition à l'alimentation DMP et consentement/non consentement à la consultation du patient

Le flux IHE PAM a été mis à jour par Interop'Santé pour intégrer la clarification de cette logique. Il est demandé que le RIS implémente cette nouvelle version du flux IHE PAM en réception et puisse l'activer dans la structure de santé qui souhaite le mettre en œuvre avec le reste du SIH.

b) Consultation du DMP / Mon espace santé

Objectifs pour le RIS en vague 2 :

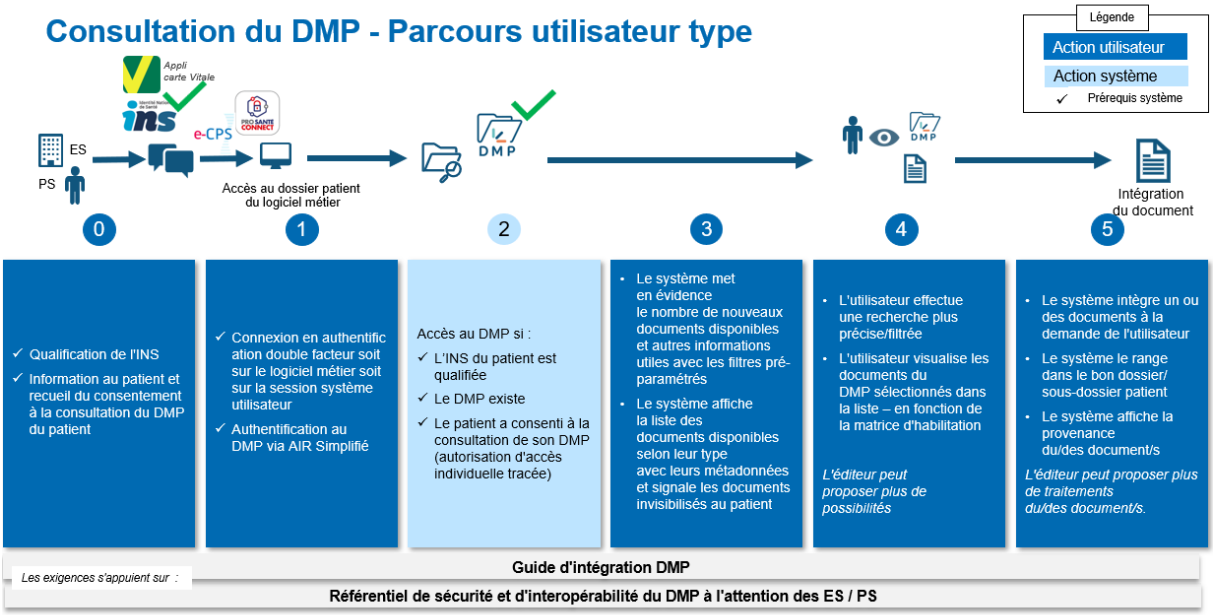
Le partage fluide et sécurisé des données de santé entre professionnels de santé et avec le patient, raison d'être du Ségur numérique, passe par la capacité pour le professionnel de consulter simplement l'information médicale présente dans l'espace santé de son patient.

Les objectifs principaux de la vague 2 sont :

- Permettre au professionnel de consulter le profil Mon espace santé du patient **directement depuis son logiciel** (par opposition à l'accès en WebPS DMP et appel contextuel) :
- Le professionnel **doit savoir sans clic s'il peut consulter le DMP / Mon espace santé de son patient.** Dans le cas où il ne peut consulter, il doit pouvoir, sur action de sa part, connaitre la ou les cause(s) de son incapacité à consulter **(cf. Conditions cumulatives explicitées ci-dessous)**.
- Le professionnel **doit connaître sans clic la provenance et le statut des documents** envoyés et intégrés (provenance, nouvelle version disponible, etc.).
- Le professionnel **doit disposer facilement du nombre de documents récemment alimentés par des professionnels et structures tiers pour orienter son choix** dans la lecture des documents.
- Le professionnel doit pouvoir examiner et rechercher/filtrer la liste des métadonnées des documents présents dans le DMP afin de pouvoir les visualiser, en mettant en avant les documents invisibles au patient.
- Le professionnel **peut manuellement intégrer un document de Mon espace santé pour le visualiser** et l'intégrer dans son logiciel.

Fonctionnalités couvertes par les exigences vague 2 :

	CONSULTATION DE MON ESPACE SANTE - Fonctionnalités périmètre Vague 2	Exigences associées
2.2	**Conformité au référentiel DMP et Information du professionnel sur le contrôle et la traçabilité des accès à Mon espace santé**	
	- Information du professionnel sur le contrôle et la traçabilité des accès au DMP / Mon espace santé via son identifiant national (RPPS) - Trace des accès aux documents provenant du DMP et extraction de ces informations - Le système DOIT être homologué CNDA correspondant au "Guide d'intégration DMP" - Homologué CNDA pour le profil consultation et alimentation avec le mode Espace de Confiance API PSC	SC.DMP/CONF.11 SC.DMP/CONF.14 SC.DMP/CONF.15 SC.DMP/PSC.40
2.3	**Autorisation de consultation du DMP et information rapide de l'utilisateur sur son contenu**	
	- Connaissance sans clic de la capacité à consulter le DMP / Mon espace santé du patient - Affichage synthétique des documents présents dans le DMP, selon des critères paramétrables par l'utilisateur - Recherche multicritères dans le DMP du patient	SC.DMP/CONF.16 SC.DMP/UX.13 SC.DMP/UX.14 SC.DMP/UX.14.BIS SC.DMP/UX.14.TER RIS.DMP/UX.15 RIS.DMP/UX.17 SC.DMP/UX.27
2.4	**Intégration de documents du DMP dans le dossier patient local**	
	- Sélection multiple de documents du DMP de la liste présentée et intégration dans le dossier patient	SC.DMP/UX.31
2.5	**Consultation par le mode "AIR" simplifié**	
	- Besoin d'une homologation CNDA pour le profil de consultation avec le mode d'authentification AIR simplifié - Lors d'une transaction, l'identifiant national (RPPS/ADELI) de l'utilisateur est systématiquement transmis	SC.DMP/AIRS.07 SC.DMP/AIRS.06



Détail des actions logicielles pour la consultation du DMP

Afin de pouvoir accéder à la consultation du DMP, plusieurs étapes sont nécessaires après l'authentification à double facteur (que ce soit sur le logiciel ou la session système utilisateur).

Cela sera possible par :

- Pro Santé Connect au travers des API en ville et dans les établissements ayant fait le choix de se tourner vers Pro Santé Connect

- AIR simplifié pour les établissements ayant fait ce choix pour le RIS et donc en cohérence avec les DPI Ségur V2 déployés à l'hôpital

Ainsi pour être référencée la solution devra implémenter ces deux modes pour interagir avec le DMP en Pro Sante Connect ou AIR simplifié suivant son contexte de mise en œuvre.

1. Tracer l'information du patient à la consultation du DMP (cf. paragraphe dédié)

Il est impératif que le patient ait été informé de cette action par le service lors de sa prise en charge, car le patient reçoit une notification au moment du premier accès à son profil. Cette notification et les traces dans Mon espace santé l'informent que le personnel médical accède à son dossier (liste des documents consultés par qui et quand), l'alimente également et qu'il peut s'opposer à ces actions s'il le souhaite. Avant toute requête au DMP, le logiciel doit s'assurer avoir tracé que le patient a bien été informé et a consenti. Si le patient n'a pas consenti à la consultation de son DMP, le logiciel ne lance aucune transaction de consultation et peut afficher cette information (sous forme d'icône) à l'utilisateur connecté.

2. Visualisation rapide de la capacité à consulter le DMP / Mon espace santé du patient

Lors de l'ouverture de l'interface "dossier patient", le système doit permettre à l'utilisateur de comprendre simplement et visuellement s'il a la capacité de consulter le DMP / MES du patient. Cette visualisation doit prendre la forme d'une icône avec 2 statuts :

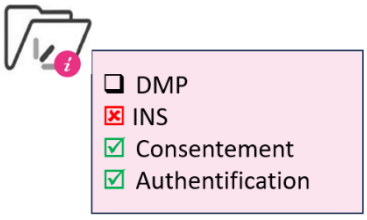
Exemples d'icônes traduisant le fait que l'utilisateur **a la capacité de consulter** le DMP / MES du patient

Exemples d'icônes traduisant le fait que l'utilisateur **n'a pas la capacité de consulter** le DMP / MES du patient

Dans le cas où l'utilisateur n'a pas la capacité de consulter le DMP / MES du patient, l'utilisateur doit pouvoir comprendre, sur action de sa part (clic sur / "mouse over" l'icône grisée), les raisons de cette incapacité. Sur la base de cette action, le système doit afficher la checklist "DICA" avec le statut de chaque condition :

- **D**MP : DMP accessible : il existe, il est ouvert, il est techniquement disponible, et le professionnel n'est pas bloqué par le patient
- **I**NS : l'INS du patient est qualifiée
- **C**onsentement : le patient a donné son consentement explicite ; celui-ci est modifiable depuis la fenêtre DICA.
- **A**uthentification : l'utilisateur est authentifié avec moyen d'identification électronique lui permettant l'accès au DMP (Pro santé Connect ou AIR simplifié avec identification 2 facteurs de l'utilisateur)

Ci-dessous un exemple d'affichage de la checklist DICA sur action de l'utilisateur :



Par ailleurs, il est très fortement recommandé d'afficher à l'utilisateur, pour chaque condition du "DICA" insatisfaite, une information avec un lien contextuel lui permettant de résoudre le problème :

DMP	Indisponibilité technique du DMP => Voir la météo du service Le DMP du patient n'existe pas. Accès bloqué par le patient.
INS	INS du patient non qualifiée => Qualifier l'INS
Consentement	Le consentement du patient n'est pas enregistré => Comment parler de MES à mon patient ? • Mon patient consent à la consultation de son DMP • J'accède en mode bris de glace
Authentification	Je ne suis pas authentifié avec un moyen d'identification sécurisé => Je me connecte avec ma CPS / e-CPS

Pour les établissements de santé, l'établissement doit avoir effectué une démarche auprès de l'Assurance Maladie afin que son FINESS (présent dans le certificat) soit bien enregistré dans la liste blanche des établissements autorisés via le mode dit AIR Simplifié. Pour cela, l'établissement doit déclarer être conforme au Référentiel de sécurité et d'interopérabilité relatif à l'accès au DMP précisant les exigences nécessaires pour être homologué et se conformer à la procédure. Le logiciel doit s'assurer que l'utilisateur s'authentifie avec deux facteurs et tracer ces informations.

Dans tous les cas, une fois que le logiciel a enregistré que le patient a consenti, lorsque l'utilisateur se connecte à l'interface où il pourra avoir les informations du DMP, il est nécessaire que le logiciel positionne automatiquement l'autorisation individuelle d'accès au DMP du professionnel à l'aide de son RPPS (en plus de l'enregistrement du FINESS de l'établissement sur la liste blanche des établissements pouvant avoir accès au DMP via le mode AIR Simplifié). L'autorisation individuelle d'accès permet au DMP de vérifier la correspondance dans le RPPS du professionnel, de vérifier que ce professionnel n'a pas été bloqué par le patient (dans Mon espace santé), tracer cette information dans le DMP et l'afficher au patient. Cette autorisation individuelle à une durée technique de 6 mois dans le DMP. Ainsi, lors des prochaines connexions, il est seulement nécessaire de vérifier son autorisation en même temps que l'existence du DMP. Au-delà des 6 mois d'autorisation technique, si l'épisode de soin se poursuit, la transaction peut être renouvelée automatiquement sans redemander aux professionnels de retracer le consentement.

Le logiciel doit rester fonctionnel lorsqu'il effectue les requêtes au DMP.

3. A l'accès à l'interface « dossier médical » selon le type de profil et le type de prise en charge, le logiciel effectue la requête sur l'existence des métadonnées avec les paramètres de date et d'auteur (acteurs tiers à l'établissement) :

Le "dossier médical" est l'espace habituellement utilisé pour lister les documents de santé du patient produits ou importés dans le système. Il ne doit pas être un espace utilisateur dédié à la seule consultation du DMP.

Régulièrement, il n'y aura rien à afficher car il n'y aura pas de nouveaux documents. Le logiciel doit tout de même permettre à l'utilisateur de rechercher des documents dans le DMP par critère.

Le logiciel affiche le nombre de documents versés au DMP du patient, sans clic supplémentaire de l'utilisateur.

Les utilisateurs notifiés sont, par défaut, les professionnels de santé et les manipulateurs en électroradiologie médicale.

Le logiciel effectue cette action de notification pour les profils utilisateurs et les types de prise en charge paramétrés. Le logiciel doit compter les documents invisibles aux patients.

L'antériorité considérée pour dénombrer les documents est définie par l'éditeur en cohérence avec le comportement préexistant du logiciel : depuis la dernière visite du patient, depuis la dernière consultation du DMP, etc…

L'ergonomie du logiciel permettant à l'utilisateur de visualiser les métadonnées de ces nouveaux documents dont le nombre est affiché est de la responsabilité de l'éditeur. Il peut notamment faire le choix :

- *D'afficher cette liste de métadonnée de manière systématiquement fusionnée avec la liste des documents (locaux) du dossier patient, avec un signe distinctif - de renvoyer l'utilisateurs vers un espace dédié à l'affichage des documents du DMP*
- *De les afficher uniquement si l'utilisateur clique sur le nombre de documents*
- *De les afficher lors du trigger "mouse over", directement dans la liste du dossier patient ou en "tooltip"*
- *Une combinaison de toutes ces possibilités, etc...*

La réinitialisation (à 0) de cette information et/ou l'acquittement de l'utilisateur sont également de la responsabilité de l'éditeur.

4. Affichage dans une liste de métadonnées *:* Si l'utilisateur le souhaite (clic), le logiciel affiche dans l'interface "dossier patient", grâce à la requête précédente, une liste des métadonnées des derniers documents afin que l'utilisateur puisse visualiser le titre et les sélectionner. Cette liste doit afficher les documents invisibles aux patients et les indiquer par un signe distinctif afin d'avertir l'utilisateur de sa présence et de l'action à effectuer (rendre visible en un clic).

5. Sélection, visualisation et intégration des documents : Dans cette liste, le logiciel permet à l'utilisateur de rechercher et sélectionner un ou plusieurs documents afin de les visualiser directement dans son logiciel, que ce soit du CDA R2 N1 ou du CDA R2 N3. Enfin, le logiciel permet à l'utilisateur de cliquer facilement sur l'intégration du ou des documents dans son logiciel. Le logiciel va enregistrer le document issu du DMP dans sa base de données en fonction de sa date, de son type, et de l'unité du responsable de l'intégration.

6. Éviter les doublons : Le logiciel doit alors vérifier que le document n'existe pas déjà dans le logiciel, sinon il ne l'intègre pas, sauf si c'est une nouvelle version ou une version supprimée afin d'éviter les doublons de documents. Pour cela, il doit s'appuyer sur la valeur des balises 'id', 'setId' et 'versionNumber' du document CDA.

7. Indiquer la provenance : Le logiciel indique d'une certaine manière (icone, texte) que le document provient du DMP / Mon espace santé, pour le distinguer des autres documents internes et externes. Cela permet en cas de doute ou de traçabilité inversées de connaître sa provenance.

Référentiel de sécurité et d'interopérabilité pour l'accès des professionnels au DMP

Le référentiel de sécurité et d'interopérabilité pour l'accès des professionnels au DMP réunit les règles applicables aux professionnels, équipes de soin et établissements de santé pour l'alimentation et la consultation du DMP. Il a été rendu opposable par arrêté après consultation de la Commission Européenne, demande de conseil à la CNIL et concertation publique.

Certaines de ces Exigences concernent *in fine* les éditeurs des LPS. Un travail a donc été réalisé pour décliner ce référentiel au sein de la vague 2 du Ségur numérique, à la fois au sein des référentiels d'Exigences applicables, et au sein du Guide d'intégration (GI) du DMP.

Mode Authentification Indirecte Renforcée (AIR) simplifié

L'accès en consultation au DMP en établissement de santé s'effectuera via une Authentification Indirecte Renforcée (AIR), avec les transactions actuelles du DMP pour la consultation.

Les éléments propres à la consultation du DMP en mode "AIR Simplifié" sont indiqués dans le Guide d'intégration du DMP et dans le Référentiel de sécurité et d'interopérabilité pour l'accès des professionnels au DMP, qui précise notamment :

- L'obligation d'une authentification en double facteur de l'utilisateur (sur logiciel ou session) ;
- La transmission systématique de l'identifiant RPPS de la personne à l'origine de la transaction, pour l'application de la matrice d'habilitation des professionnels (conditions d'accès en lecture aux types de documents selon la profession ou la discipline), la traçabilité des accès et la détection des mésusages potentiels.
- Les conditions d'homologation des établissements pour l'utilisation du mode "AIR simplifié"

c) Alimentation du DMP / Mon espace santé

Objectifs pour le RIS en vague 2 :

En vague 1, l'objectif a été de généraliser l'envoi systématique et sécurisé dans le DMP de la copie numérique des documents de santé communiqués au patient, en format CDA et en utilisant les types codes de la matrice d'habilitation du DMP.

L'objectif de la vague 2 est de :

- **Renforcer le caractère systématique de l'alimentation du DMP**, avec la capacité à de retenir l'envoi d'un document spécifique au sein du logiciel avant la validation, l'exécution de l'envoi dès que possible une fois le document validé, en différant l'ordre d'envoi lorsque nécessaire
- Permettre **d'alimenter ponctuellement** des documents présents dans le logiciel métier datant d'épisodes de santé antérieurs dit « historiques » n'ayant pas été préalablement envoyé au DMP, sous condition d'avoir au préalable qualifier l'INS du patient.
- S'assurer que la fonction de suppression des documents dans le DMP soit effective, sur demande du patient, sur erreur de patient ou suppression définitive du document dans le logiciel producteur.

Fonctionnalités couvertes par les exigences vague 2 :

	ALIMENTATION DE MON ESPACE SANTE - Fonctionnalités périmètre Vague 2	Exigences associées
2.6	**Alimentation systématique de Mon espace santé**	
	- Envoi systématique et automatique sans action utilisateur des documents au DMP avec une exécution différée et en tâche de fond. - Possibilité pour l'utilisateur de bloquer ou annuler l'ordre d'envoi au DMP avant sa validation et pendant la période de différée d'exécution. - Mise en attente des documents lorsque la connexion au DMP n'est pas possible puis exécution des ordres d'envoi lorsque la connexion est rétablie. - Homologation du Système conformément au profil alimentation en authentification indirecte	SC.DMP/ALI/PROG.02 SC.DMP/ALI/PROG.03 SC.DMP/ALI/PROG.05 SC.DMP/ALI/PROG.06 SC.DMP/ALI/PROG.07 SC.DMP/CONF.19
2.7	**Alimentation ponctuelle de Mon espace santé**	
	- Possibilité d'ajouter au DMP des documents datant d'épisodes de santé antérieurs sous condition d'avoir l'INS qualifiée du patient et avec certaines caractéristiques (date, auteur, CDA) - Ajout manuel dans le DMP des documents qui n'ont pas encore été alimentés avec succès	SC.DMP/HISTO.03 SC.DMP/HISTO.04 SC.DMP/HISTO.05
2.8	**Suppression d'un document du DMP**	
	- Possibilité de supprimer un document du DMP en cas d'erreur d'alimentation ou de demande du patient concerné	SC.DMP/CONF.03

d) Remise en visibilité des documents du patient dans le DMP / Mon espace santé

Objectifs pour le RIS en vague 2 :

Le Dossier médical de Mon espace santé permet aux professionnels d'alimenter les documents de façon invisible aux patients et/ou à ses représentants légaux. Cela permet une coordination entre les professionnels de santé avant que le patient n'ait connaissance des informations sensibles du document. Ces informations doivent être dévoilées lors d'une consultation d'annonce effectuée par un professionnel de santé avec le patient.

Ainsi, le logiciel doit alors :

- Permettre au **professionnel qui produit le document nécessitant une consultation d'annonce de le rendre facilement invisible lors de l'alimentation du DMP**
- Permettre de **transmettre aux correspondants par MSS l'information que le document qui leur est transmis a été alimenté en invisible en DMP** et nécessite une consultation d'annonce ainsi qu'une remise en visibilité au patient.

Exemple de texte informant un correspondant que le document qui leur est transmis a été alimenté en invisible en DMP à introduire dans le corps du message MSS :

> *"Veuillez trouver ci-joint le document [nom du document] concernant [Nom prénom]. Ce document vous est adressé en tant que prescripteur et/ou médecin traitant.*
>
> *Pour information, **ce document a été également envoyé dans l'espace santé (DMP) du patient en "invisible**" car il contient potentiellement des informations devant être apportées à sa connaissance avec un accompagnement médical.*
>
> *Ce document nécessite donc votre attention et un suivi de prise en charge ou une **annonce pour la personne concernée**.*
>
> *Une fois que ce suivi ou cette annonce a été effectuée, nous vous invitons à remettre le document en 'visible' directement dans le DMP/Mon espace santé. Cela permettra un meilleur accompagnement du patient et lui permettra d'accéder aux informations présentes sur le document. En effet, si ce n'est pas fait, la personne concernée sera informée au bout d'un mois qu'elle dispose d'un document 'invisible' dans son espace santé et sera à nouveau encouragée à venir vous consulter. Au bout de trois mois, le document sera automatiquement rendu visible pour éviter toute perte d'information pour le patient."*

- Permettre au **professionnel qui réalise la consultation d'annonce de remettre en visibilité le document** « manuellement » directement dans son logiciel habituel, en facilitant la mise en évidence au professionnel des documents « invisibles »
    - Afficher à l'aide d'un signe distinctif les documents qui sont invisibles au patient et ses représentants légaux dans la liste des métadonnées des documents.
    - Afficher le critère des documents invisibles au patient dans la fonction recherche des documents du DMP.

Fonctionnalités couvertes par les exigences vague 2 :

	INVISIBILISATION DE MON ESPACE SANTE - Fonctionnalités périmètre Vague 2	Exigences associées
2.9	**Rendre facilement invisible un document alimentant le DMP et en informer les correspondants**	
	- Possibilité, en 1 clic, de rendre invisible un document au patient avant sa validation et son envoi au DMP. - Transmettre à un professionnel de santé par MSS, un message paramétrable l'informant que ce document a été envoyé en invisible au DMP et nécessite une annonce.	SC.DMP/UX.51 SC.MSS/UX.35
2.10	**Autorisation de consultation du DMP et information rapide de l'utilisateur sur son contenu**	
	- Affichage des documents qui sont invisibles au patient et / ou représentants légaux et possibilité de les rendre visible à l'un et/ou à l'autre. - Information directement disponible dans l'interface du « dossier médical » du nombre de documents qui ont été versés au DMP dont les documents invisibles (au patient). - Fonction de recherche et/ou de filtrage basée sur des critères issus des métadonnées XDS du DMP (documents invisibles, période donnée…).	SC.DMP/UX.14.BIS RIS.DMP/UX.15 SC.DMP/UX.27

Rappel des fondamentaux concernant la mise en visibilité et remise en visibilité des documents alimentés au DMP

A l'issue de nouvelles concertations avec les associations de patients, professionnels et établissements représentants, il a été acté le maintien du mécanisme d'invisibilisation au sein du DMP avec comme enjeux de s'assurer :

- De minimiser les cas d'invisibilisation aux stricts documents dont la sensibilité du contenu justifie un accompagnement humain ;
- Qu'aucun document ne sera masqué au patient de manière pérenne à son insu ;
- Que le patient soit informé si un document sensible n'est pas mis en visibilité par un professionnel de santé après un certain délai ;
- Qu'*in fine* ce dernier aura accès au document avec une remise en visibilité automatisée au niveau de Mon espace santé au bout d'un certain temps. Cela permet de garantir la pleine connaissance du patient pour agir au cas où la consultation d'annonce n'aurait pas pu avoir lieu.

Un mécanisme encadre historiquement le fonctionnement du DMP pour gérer ces situations qui nécessitent au préalable un dispositif d'annonce. Les textes de loi L. 1111-2 et L. 1111-15 du code de la santé publique encadrant ce mécanisme prévoient 3 fonctions pour gérer la complexité spécifique de ces situations. Ainsi, le dispositif a été réaffirmé pour faciliter ces fonctions nécessaires et complémentaires et gérer la complexité spécifique de ces situations et en adaptant les délais à la réalité des usages :

- Un **mode d'envoi par l'acteur de santé auteur du document invisible au patient** mais **consultable par les professionnels habilités** ;
  - *Une liste indicative de la **typologie de documents à alimenter avec précaution** est mise à disposition des professionnels et établissements, à adapter par les établissements, en concertation avec l'avis des communautés médicales concernées qui tiendra compte des organisations et prises en charge spécifiques (exemples du VIH, de l'anapath, de la gynécologie…) au sein du document "Fondamentaux et principes opérationnels d'échange et de partage des données de santé".*
  - *Au-delà de ces règles générales, une adaptation des modalités d'envoi et de visibilité devra pouvoir être réalisée au cas par cas, à l'échelle individuelle du document, sur décision médicale.*
- Des logiciels qui permettent au **professionnel qui réalise la consultation d'annonce** de **remettre en visibilité le document** « manuellement » directement dans son logiciel habituel ;
- Une « **remise en visibilité automatique » par le DMP de tous les documents invisibles aux patients prévue 3 mois après l'envoi du document,** avec une information préalable du patient au **bout de 1 mois** sur l'existence d'un document invisible dans son DMP qui nécessite une consultation d'un professionnel. Le délai de 3 mois, très supérieur aux délais habituels des annonces, a été retenu afin de maximiser les chances que les personnes bénéficient d'une information préalable sur le contenu du document, accompagnée par un professionnel de santé.

3.2.3 Gestion de la MSSanté

Objectifs pour le RIS en Vague 2 :

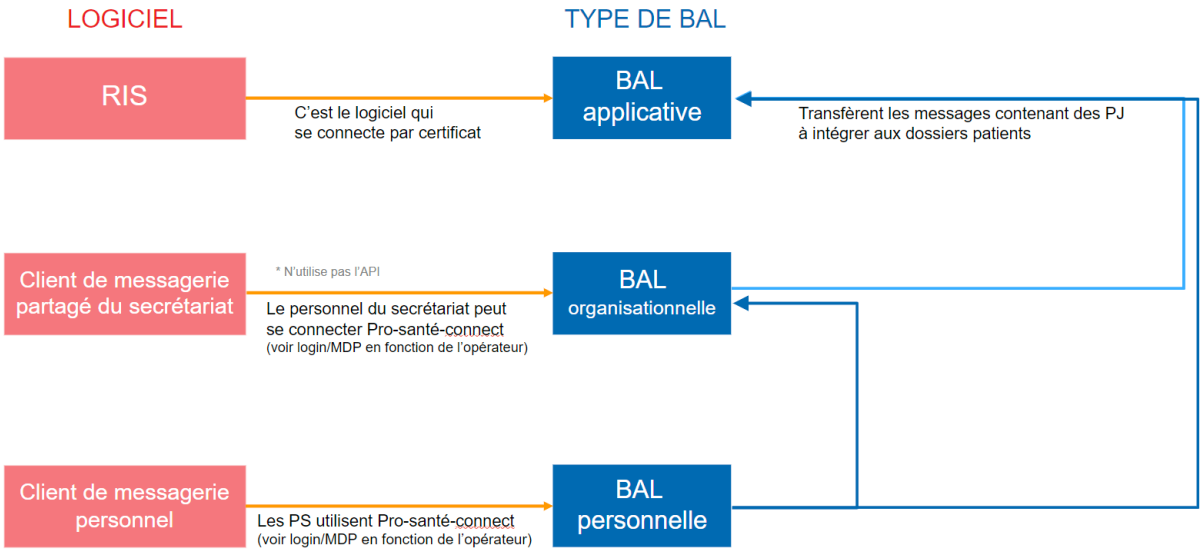
La messagerie sécurisée de santé (MSSanté) est la modalité préférentielle d'échange des documents de santé entre les professionnels de santé. Dans la suite de la vague 1, qui a permis de développer significativement l'envoi par MSSanté des documents à destination des professionnels de santé et des patients, la vague 2 vise en particulier les objectifs suivants :

- Automatiser au maximum l'intégration des documents de santé reçus en établissement par MSSanté lorsque les identités nationales de santé se correspondent.
- Permettre de gérer les remplacements et suppression des documents reçus par MSSanté.

Fonctionnalités couvertes par les exigences vague 2 :

	Gestion de la MSSanté - Fonctionnalités du périmètre Vague 2	Exigences associées
3.1	**Envoi sécurisé vers la messagerie de Mon espace santé d'un patient**	
	- Fermeture du canal de communication avec le patient après envoi du message via ou sans une PFI	SC.MSS/CONF.24 SC.MSS/CONF.21
3.2	**Facilitation de l'interrogation de l'annuaire santé**	
	- Recherche multicritère l'adresse MSSanté d'un correspondant en interrogeant l'annuaire MSSanté depuis le RIS	SC.MSS/UX.10
3.3	**Intégration et gestion des documents reçus par MSSanté**	
	• Impact de la demande de mise à jour ou suppression d'un document CDA reçu par MSSanté dans le logiciel avec visibilité du précédent document. • Envoi aux destinataires de la MSSanté via la fonction PFI de la mise à jour ou suppression d'un document CDA généré par le système • Informer l'utilisateur et les correspondants des documents nouveaux ou mis à jour reçus par MSSanté • Importation manuelle des documents CDA contenus dans l'enveloppe IHE.XDM et exploitation des métadonnées du document CDA • Génération d'un courriel MDN en cas d'échec d'intégration	SC.MSS/UX.05 SC.MSS/UX.05.BIS SC.MSS/UX.38 SC.MSS/UX.39 SC.MSS/UX.11
3.4	**Intégration automatique d'un document reçu par MSSanté grâce à l'INS qualifiée**	
	- Intégration automatique des documents dont l'INS qualifiée correspond exactement - Information aux utilisateurs de la présence de nouveaux documents intégrés au systèmes et issus d'un courriel MSS	SC.MSS/UX.07 SC.MSS/UX.40
3.5	**Production et conservation de traces MSSanté**	
	- Traçage de l'ensemble des flux de transmissions et d'actions effectuées sur les documents reçus par MSSanté jusqu'à leur traitement (intégration, remplacement, suppression).	SC.MSS/UX.37 SC.MSS/CONF.17 SC.MSS/CONF.18
3.6	**Interopérabilité avec les opérateurs de MSSanté**	
	-Utilisation de protocoles standardisés et sécurisés pour l'échanges de données par MSSanté - Standardisation de la cinématique de connexion à une BAL MSSanté - Positionnement des-têtes SMTP (invisibles de l'utilisateur) exploités par l'ANS à des fins statistiques : présence d'un INS qualifié, identifiant du logiciel référencé Ségur émettant le message, type de document CDA échangé - interface d'accès aux BAL en utilisant le protocole IMAP 4 (rev1 ou rev2) conformément à la RFC 3501 ou RFC 9051 - Demande d'ouverture de connexion SMTP et IMAP sur l'interface BAL personnelle ou organisationnelle de l'API LPS d'un Opérateur MSSanté - Refresh du token PSC et déclenchement de la fin de session avec le système de messagerie de l'opérateur MSSanté -Réouverture automatique d'une session IMAP et SMTP -Recherche dans l'annuaire santé d'une adresse MSSanté pour envoi de courriels depuis une bal perso ou organisationnelle - Acceptation uniquement d'un certificat issu de IGC Santé gamme Elémentaire Organisation pour se connecter à une l'interface API LPS -Règle de Mémorisation de l'Access Token PSC -Capacité d'identifier les courriels reçus via MSSanté avec archive zip au format IHE XDM en pièce jointe.	SC.MSS/CONF.01 SC.MSS/CONF.03 SC.MSS/CONF.05 SC.MSS/CONF.06 SC.MSS/CONF.07 SC.MSS/CONF.08 SC.MSS/CONF.10 SC.MSS/CONF.11 SC.MSS/CONF.12 SC.MSS/CONF.14 SC.MSS/CONF.15 SC.MSS/CONF.16 SC.MSS/CONF.20 SC.MSS/CONF.22 SC.MSS/CONF.27 SC.MSS/CONF.28 SC.MSS/UX.01

Organisation des boites de messagerie pour cabinet d'imagerie médicale



BAL organisationnelle :

- Adresse à diffuser pour les correspondants extérieurs (publiée dans l'annuaire national)
- Utilisée par le secrétariat :
- Pour les échanges avec les correspondants professionnels
- Car c'est le point de contact par défaut avec les patients et les correspondants (c'est l'email « reply to » inscrit dans tous les CR et dans « reply-to » de la BAL applicative lors des envois)

BAL applicative :

- Adresse à NE PAS diffuser à l'extérieur (publiée en liste rouge de l'annuaire national)
- Connectée au RIS, et utilisée pour 2 usages :
- L'envoi automatique des comptes rendus aux patients comme aux professionnels correspondants
- L'intégration de documents sous forme de liste de travail

BAL personnelle :

- Adresse à diffuser à l'extérieur selon le choix du professionnel
- Utilisée par le PS pour traiter « en direct » avec les professionnels de santé (dans certains cas avec les patients)

Cas d'usage et explication de l'intégration par le RIS des documents reçus par MSSanté et transmis par la PFI au RIS

Dans ce chapitre, la fonctionnalité métier principale apportée par la vague 2 est **d'automatiser l'intégration des documents reçus dans une boîte aux lettres (BAL) Applicative** opérée par la fonction PFI, qui transfère le contenu du message et le document à la fonction RIS, laquelle intègre le document quand elle détecte une correspondance entre les INS qualifiées du document et de la base patients du RIS.

La vague 2 va permettre de mettre en œuvre les cas d'usage du document « Catalogue des usages MSSanté » publié par l'ANS, et qui nécessitent l'intégration de documents envoyés en pièces jointes dans le système destinataire. Deux catégories de cas d'usage ont été identifiés :

- **Echange et intégration automatique de documents lorsqu'ils sont envoyés à une BAL personnelle ou organisationnelle**. Les courriels sont consultés par un professionnel via un client de messagerie, intégré ou non au système destinataire. Cela correspond par exemple au deuxième cas d'usage du catalogue précité (Transfert d'un patient d'un CH vers un autre CH), également décrit dans le volet *Transmission de documents CDA en HL7v2*. La vague 2 propose une méthode pour intégrer automatiquement les pièces jointes dans le RIS. Comme BAL personnelles et organisationnelles ne sont pas connectés au RIS de l'établissement, le scénario d'intégration prévoit que les courriels MSSanté qui contiennent des pièces jointes IHE_XDM soit transférés manuellement ou

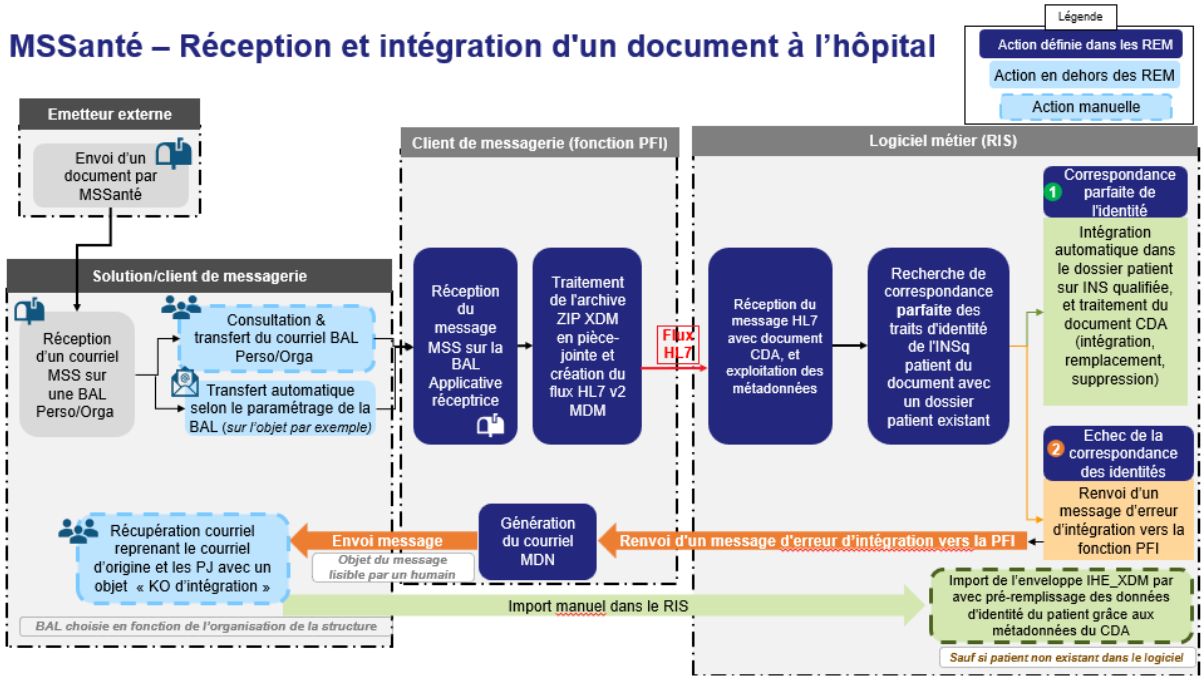
automatiquement vers des BAL applicatives associées à des services cliniques (par exemple), sur correspondance de l'ensemble des traits d'identités des INS qualifiées.

- **Echange et intégration automatique de documents entre un RIS (système source) et un système destinataire (par exemple un DPI).** Les échanges se font via des BAL applicatives et sont réalisés sans intervention spécifique des professionnels de santé. Ces échanges sont équivalents aux échanges de données via des messages HL7 ORU et MDM, mais le vecteur de communication est un courriel. Cela correspond au cas d'usage « Envoi/réception d'un CR de biologie médicale » du catalogue, qui est décrit dans son ensemble dans le volet *Transmission de document(s) CDA en HL7v2*.

Ainsi, la demande de traitement sur le document, incluse dans le courriel MSSanté reçue via la BAL Applicative, est transformée par la fonction PFI en un message HL7 v2 MDM (flux d'interopérabilité standardisé), transmis au RIS qui réceptionne ce message HL7.

Le référentiel INS [Exigence 11] précise qu'en cas de réception d'une INS non préalablement qualifiée par le destinataire, ce dernier doit effectuer la qualification. Le guide d'implémentation précise que lors de la réception d'une INS non présente au statut qualifié ou récupéré, alors le système doit faire un appel de récupération auprès du téléservice INSi, et mettre en cohérence les traits reçus et ceux présent dans le SI local (cf. Paragraphe : **Permettre aux professionnels de bénéficier sous conditions de l'INS transmise par un tiers de confiance du** présent document**).**

Les spécifications des messages HL7 et des courriels MDN des volets « Transmission de documents CDA en HL7v2 » et « Transmission au LPS d'un document CDA provenant d'un courriel MSSanté » détaillées peuvent permettre de concevoir d'autres scénarios d'intégration spécifiques à des organisations particulières.



Exemple : Détails des étapes de l'intégration des documents non intégrés automatiquement

- *Un message ayant comme pièce jointe une archive IHE_XDM est réceptionné dans une BAL organisationnelle.*

Par paramétrage du client de messagerie utilisé par les utilisateurs, il est possible d'automatiser que certains documents soient transférés sur une BAL App choisie. Un exemple de règle serait : si un courriel arrive dans une BAL (ORGA) et qu'il contient une pièce jointe IHE_XDM.ZIP ou un objet formaté (XDM/1.0/DDM+<libellé> <NOM> <prénom> <date de naissance>), ce courriel peut être transféré

automatiquement vers une autre BAL (par exemple, la BAL APP du service correspondant à la BAL ORG). L'émetteur du courrier transféré peut être le destinataire du courrier original, c'est-à-dire l'adresse de la BAL organisationnelle.

- *Le serveur de messagerie transmet le message MSSanté à la BAL Applicative.*
- *La fonction PFI, client de messagerie MSSanté, lit le message dans la BAL applicative, transforme le courriel MSSanté en flux HL7 v2 MDM et envoie ce flux HL7 v2 MDM au RIS.*
- *Le RIS réceptionne le message du flux HL7 et exploite les données du message HL7 et de l'entête du document CDA.*
- *Le connecteur entrant du RIS peut prévoir un paramétrage pour associer une adresse mail à un service de l'établissement et classer plus finement le document dans le dossier du patient (recherche d'un séjour associé au service par exemple).*
- *Le RIS compare l'INS qualifiée du document avec les INS qualifiées de sa base patients sur l'ensemble des 5 traits d'identité et du matricule INS. S'il y a non-correspondance des INS (si le patient n'est pas trouvé) alors le DPI renvoie vers la fonction PFI un message d'erreur (accusé de réception HL7 v2 ACK)*
- *La fonction PFI reçoit le message d'erreur HL7 de façon synchrone du RIS avec précision du code et du libellé de l'erreur.*
- *La fonction PFI créé un nouveau courriel MSSanté (de type MDN) vers l'espace de confiance MSSanté vers la BAL organisationnelle (décrit dans le volet du CI-SIS)*
- *Le serveur de messagerie transmet le courriel MDN vers la BAL organisationnelle d'origine.*
- *Dans son client de messagerie usuel, l'utilisateur consulte sa BAL organisationnelle pour y retrouver le courrier MDN qui reprendra le courriel d'origine et les pièces jointes. Un paramétrage du client de messagerie peut permettre de mettre dans un dossier particulier les mails en erreur*
- *L'utilisateur du RIS importe manuellement le(s) document(s) CDA du fichier IHE_XDM.zip dans le RIS (et non le(s) fichier(s) PDF). Le RIS exploite les métadonnées pour pré-remplir la recherche patient (recherche habituelle du RIS pour sélection manuelle du patient et rangement dans le dossier.*

3.2.4 Identification électronique & Pro Santé Connect

Objectifs pour le RIS en vague 2 :

L'identification électronique des acteurs est un **préalable indispensable au partage fluide et sécurisé des données de santé**. Depuis plusieurs années, les pouvoirs publics déploient le moyen d'identification électronique Pro Santé Connect (PSC) pour les acteurs de la santé. Pro Santé Connect est un fédérateur de fournisseurs d'identité au standard OpenID. Pro Santé Connect permet aux professionnels de santé de s'identifier grâce à plusieurs moyens d'authentification électroniques, tels que la e-CPS (application mobile) ou la carte CPS physique, à tous les services numériques de santé raccordés à Pro Santé Connect.

L'objectif est de pouvoir **simplifier l'identification électronique des professionnels** afin de limiter les étapes d'authentification aux services numériques en santé, avec PSC et/ou avec d'autres systèmes de Single Sign-on (SSO). Par conséquent, il est souhaité de généraliser l'authentification par PSC pour l'accès aux services numériques en santé, notamment les services socles : MSSanté, DMP, …

- Pour les RIS, il s'agit de proposer aux Professionnels de Santé une identification simple, sécurisée et unifiée – où les Professionnels de Santé peuvent se connecter aux services socles, en passant de l'un à l'autre de manière fluide, sans réidentification via les fonctionnalités de navigateur ;
- Les services déléguant leurs authentifications à Pro Santé Connect bénéficient de l'image de confiance et de sécurité associée à Pro Santé Connect – Pro Santé Connect proposant des authentifications sur une base locale de comptes reposant sur le protocole OpenID Connect.

Fonctionnalités couvertes par les exigences vague 2 :

	Identification électronique & Pro Santé Connect - Fonctionnalités du périmètre Vague 2	Exigences associées
4.1	**Authentification et connexion sécurisée aux services socles par Pro Santé Connect**	
	- Identification de l'utilisateur sur le Système avec Pro Santé Connect au moins par l'une des 2 modalités suivantes : - dans le cas d'un client léger : mode web ; - dans le cas d'un client lourd application native avec renvoi vers navigateur externe. - A la 1ère connexion avec PSC, rapprochement du compte utilisateur authentifié avec PSC avec un (ou plusieurs) compte (s) éventuellement préexistant(s). - Authentification par défaut avec Pro Santé Connect - Usage de Pro Santé Connect pour la connexion au service socle sans réidentification. - Configuration de l'intégration de Pro Santé Connect en tant que client lourd en utilisant CIBA - Incitation à la connexion au LPS via PSC afin d'offrir d'emblée au médecin l'accès à tous les services nécessitant cette authentification	SC.PSC.01 SC.PSC.02 SC.PSC.15 SC.PSC.08 SC.PSC.13 (profil CIBA) SC.PSC.15
4.2	**Authentification sur une base de comptes locale via OIDC**	
	- Possibilité de choisir entre au moins deux fournisseurs d'identités compatibles OIDC dont l'un doit être Pro Santé Connect.	SC.SSI/IAM.80
4.3	**Habilitations à l'Espace de confiance (EDC) Pro Santé Connect**	
	Habilitation Editeur de logiciel utilisateur à se connecter à l'espace de confiance (EDC) Pro Santé Connect Habilitation Editeur de Proxy e-santé à se connecter à l'espace de confiance (EDC) Pro Santé Connect	SC.PSC.14 SC.PSC.16

Pour en savoir plus sur l'implémentation du standard OpenID Connect, consultez-la documentation technique Pro Santé Connect.

Identification électronique CIBA (profil optionnel) :

Si l'Editeur le souhaite, en complément des exigences du profil Général, il peut choisir de mettre en œuvre une authentification en Client Initiated Backchannel Authentication (CIBA) dans le cas d'un client lourd, conformément au référentiel Pro Santé Connect.

Pour en savoir plus sur l'implémentation des flux CIBA, consultez-la documentation CIBA Pro Santé Connect.

Rappels réglementaires sur l'identification électronique

- Référentiel d'identification électronique, rendu opposable par l'arrêté du 28/03/2022
- Référentiel Pro Santé Connect, rendu opposable par arrêté du 4/04/2022
- Implémentation de Pro Santé Connect obligatoire depuis le 01/01/2023 pour les services numériques sensibles
- Enregistrement au RPPS de tous les professionnels ayant besoin d'accéder aux SNS (via PSC) - Arrêté du 23/09/2022
- Référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au DMP, rendu opposable par l'arrêté du 26/10/2023

Espace de confiance PSC et API Pro Santé Connect :

En vague 2, l'objectif est de généraliser l'authentification par PSC pour accéder aux services numériques en santé, notamment les services socles : MSSanté, DMP, INSi et l'Ordonnance Numérique.

Dans cet objectif, un « Espace de Confiance Pro Santé Connect » a été défini aboutissant à l'apparition d'une nouvelle notion « d'API Pro Santé Connectée » introduite dans le CI-SIS volet transport du 5 juin 2023.

Pour les LPS, il s'agit de proposer aux Professionnels de Santé une identification simple, sécurisée et unifiée – où les Professionnels de Santé peuvent se connecter aux services socles et accéder à des données de santé, de manière fluide, sans réidentification via les fonctionnalités de navigateur.

Espace de Confiance PSC

L'Espace de Confiance PSC permet d'ouvrir la connexion par API Pro Santé Connectée aux services socles du numérique en santé, notamment les téléservices de l'Assurance Maladie (dans un 1er temps : DMP, ON, INSi). Il définit des règles permettant une relation de confiance entre ses différents composants afin de garantir un niveau de sécurité minimal et renforcé.

L'architecture repose sur la mise en œuvre d'un serveur intermédiaire Proxy e-santé destiné à sécuriser les échanges de données entre le Fournisseur de Service Utilisateur et l'API Pro Santé Connectée.

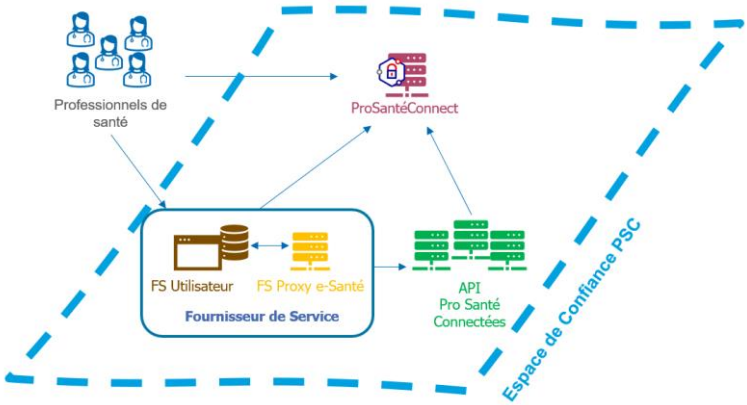


Schéma simplifié de l'Espace De Confiance (FS Proxy e-santé et FS Utilisateur)

L'EDC permet la mise en place d'un échange de flux permettant aux professionnels de santé d'accéder aux données fournies par une API Pro Santé Connectée de manière transparente et fluide à partir de la connexion sécurisée de PSC.

Dans le cadre de l'EDC, un industriel peut prétendre à supporter jusqu'à 4 rôles différents cumulables au dans l'Espace de Confiance PSC :

- **Editeur de Logiciel Utilisateur** : rôle tenu par le responsable du développement, de la maintenance du logiciel utilisateur depuis son architecture jusqu'à son code source. Le logiciel utilisateur a pour caractéristique principale de fournir à l'utilisateur final une interface homme-machine métier adaptée à son exercice professionnel.
- **Editeur de Proxy e-Santé** : rôle tenu par le responsable du développement, de la maintenance d'un Proxy e-Santé depuis son architecture jusqu'à son code source.
- **Opérateur de Service Utilisateur** : rôle tenu par le responsable du déploiement d'un logiciel utilisateur au sein d'un écosystème technique et d'utilisation ciblé par l'opérateur lui-même, fournissant ainsi un Service Numérique dans un environnement de production à des Utilisateurs et habilitée à utiliser PSC conformément aux Conditions Générales d'Utilisation PSC. Ce rôle s'appuie directement sur ceux de l'Editeur de Logiciel Utilisateur ainsi que sur celui de son Opérateur de Proxy e-Santé.
- **Opérateur de Proxy e-Santé** : rôle tenu par le responsable du déploiement d'un Proxy e-Santé au sein d'un écosystème technique ciblé par l'opérateur lui-même, fournissant ainsi en production un Service Numérique constitué uniquement du serveur intermédiaire Proxy e-Santé. Ce rôle s'appuie directement sur celui de l'Editeur de Proxy e-Santé.

Chaque candidat peut porter l'un ou plusieurs de ces rôles suivant son souhait et la construction de son offre industrielle. Ainsi, un candidat au rôle d'Opérateur de Service Utilisateur peut choisir de développer son propre Proxy e-Santé et de l'opérer lui-même ensuite alors qu'un autre peut choisir de s'appuyer sur un partenariat avec un Opérateur de Proxy e-Santé.

Obligations pour obtenir le présent référencement Ségur

Dans le cadre du présent référencement Ségur, l'Editeur doit implémenter dans sa Solution logicielle l'appel aux API Pro Santé Connectées conformément au référentiel « Pro Santé Connect Communauté – Extension Espace de confiance ».

Pour cela, il est nécessaire :

- D'obtenir l'habilitation Espace de Confiance API PSC **Editeur de logiciel utilisateur**, ce qui implique en particulier le passage avec succès du **test d'intrusion Editeur de logiciel Utilisateur.**
- D'obtenir l'habilitation Espace de Confiance API PSC **Editeur de Proxy e-santé**, ce qui implique en particulier le passage avec succès du **test d'intrusion Editeur de Proxy e-santé.**

NB : afin de bénéficier du dispositif de financement décrit dans l'AF-IMG-RIS-Va2, l'industriel devra également disposer de l'habilitation « Opérateur de service utilisateur » de l'espace de confiance Pro Santé Connect.

Pour aider le candidat à préparer les développements et obtenir l'habilitation Espace de Confiance PSC, il est recommandé de s'approprier la documentation disponible dans l'ordre suivant :

Espace de confiance PSC		
1	Définition de l'espace de confiance, des fournisseurs de service et fournisseur de données Exigences de l'espace de confiance Prosanté connect à respecter et préconisations pour un Fournisseur de Service (FS) ou un Fournisseur de données (FD) souhaitant implémenter PSC ou l'appel à une API Pro Santé Connectée	Référentiel Espace de confiance Pro Santé Connect
Spécifications techniques		
2	Volet transport du CI-ISIS pour les APIs PSC décrit la sécurisation des flux génériques d'une API PSC (openid connect/OAUTH2 token exchange/mTLS spécification des protocoles de transport à utiliser pour les flux entre : • un système cible offrant une API Pro Santé Connectée à laquelle il est possible de se connecter de façon synchrone et : • un système initiateur, pouvant être une application web serveur, une application client lourd, une application mobile native ou web, se connectant à une API Pro Santé Connectée de façon synchrone.	Spécifications d'interopérabilité API REST
3	Volet transport AMO des TLSi décrit la couche transport historique avec l'assertion PS (SAML), cette assertion est toujours exigée dans l'API PSC : cadre d'interopérabilité des TLSi de l'AMO.	Intégrer un TLSi AMO (documents communs)
4	Guides d'intégration pour chaque Téléservice INSi, DMPi, ON et Messagerie Sécurisée de Santé avec l'API PSC : description des éléments d'authentification spécifiques au service.	Guides d'intégration Téléservice
Habilitation espace de confiance API PSC : contrôles, preuves et tests d'intrusion		
5	Tests d'intrusion Editeur de logiciel utilisateur – Imagerie	Documents disponibles sur la page Espace de confiance API Pro Santé Connectées
6	Test d'intrusion Editeur de logiciel Proxy e-santé	
7	Fichier point de contrôles : détaillant les points de contrôles par exigences	
8	Document de conformité : document permettant d'évaluer la conformité aux exigences et les preuves à fournir dans le cadre de la candidature à l'EDC Pro Santé Connect.	
9	Processus bac à sable permettant aux éditeurs de logiciel utilisateur d'accéder aux environnements de tests bac à sable CNDA avant l'ouverture du guichet PSC Espace de confiance	
10	Parcours de raccordement à l'espace de confiance PSC	

3.2.5 Sécurité des SI

Objectifs pour le RIS en vague 2 :

Afin de renforcer les points sensibles identifiés à la suite du questionnaire de la vague 1 et en tenant compte des incidents survenus en 2022 et 2023, un ensemble d'exigences de sécurité réparties en trois thématiques principales ont été élaborées :

- Le **Socle Commun** englobant des exigences techniques et organisationnelles visant à garantir le respect des règles de base de la sécurité des systèmes d'information ;
  - Une gouvernance efficace pour sécuriser de manière proactive les solutions, assurer la conformité réglementaire et gérer efficacement les risques de la SSI ;
  - Un renforcement de la sécurité du développement logiciel, notamment par l'application de bonnes pratiques cyber tant pour la conception de nouveaux produits que pour l'intégration de nouvelles fonctionnalités ;
  - Un maintien en conditions de sécurité des solutions grâce à un processus d'identification des vulnérabilités qui comprend des tests d'intrusion, une veille sur les menaces émergentes et une gestion proactive des correctifs de sécurité ;
  - La mise en œuvre de mesures correctives et préventives pour remédier aux vulnérabilités critiques les plus fréquentes qui pourraient être exploitées par des attaquants.
- Des **exigences IE (identification électronique)** qui visent à prendre en compte la réglementation décrite dans le référentiel d'identification électronique qui est applicable lorsque le logiciel utilise une interface utilisateur, pour renforcer la sécurité des connexions aux solutions fournissant des services numériques qui traitent des données de santé et pour une amélioration de la gestion des comptes grâce à des exigences de sécurité régissant la gestion des identités et des droits d'accès ;
- Des **exigences IAM** (Identity and Access Management) spécifiques aux solutions hospitalières et conçues pour répondre au besoin d'intégration simplifiée aux systèmes des solutions de SSO (Single Sign-On) et d'IAM.

Fonctionnalités couvertes par les exigences vague 2 :

	SECURITE DES SI - Fonctionnalités périmètre Vague 2	Exigences associées
5.1	**Démarche SSI chez l'éditeur de la solution logicielle**	
	Identification des responsables de la sécurité et formalisation de leurs rôles et responsabilités. Sensibilisation des équipes aux enjeux et aux risques liés à la sécurité des systèmes d'information. Mise à disposition d'un standard ou guide de bonnes pratiques visant à garantir la sécurité des développements, à la fois lors de la conception du produit ou de l'ajout de nouvelles fonctionnalités Réalisation d'une veille technologique continue autour des menaces émergentes.	SC.SSI/GEN.01 SC.SSI/GEN.02 SC.SSI/GEN.03 SC.SSI/GEN.11 SC.SSI/GEN.20
5.2	**Gestion des comptes, des permissions et des sessions des administrateurs et des utilisateurs**	
	Synchronisation régulière des données de la base de comptes avec le fournisseur d'identité ou le référentiel local (annuaire AD/LDAP de l'établissement de santé). Renforcement de la sécurité des comptes à privilèges par l'application d'une politique de mot de passe incluant différents critères tels que la longueur minimale, les délais d'expiration, le blocage des comptes, etc. Possibilité d'extraire les données de comptes afin de permettre la revue et mise à jour de ces éléments par l'administrateur Permettre aux établissements d'utiliser le fournisseur d'identités de leur choix (compatibilité du système avec le standard Open Id Connect et le flux Authentification Code Flow)	SC.SSI/IAM.83 SC.SSI/IAM.92 SC.SSI/IAM.94 SC.SSI/IAM.80
	Sécurisation des processus de gestion des attributs d'identité, lors de la création que de la modification des attributs d'identité.	SC.SSI/IE.56 SC.SSI/IE.57 SC.SSI/IE.33
	Renforcement de la sécurité des comptes, notamment lors de la connexion et de la déconnexion des systèmes.	SC.SSI/IE.36 SC.SSI/IE.38 SC.SSI/IE.39
5.3	**Gestion des sauvegardes**	
	Elaboration et l'application d'un processus de sauvegarde et de restauration.	SC.SSI/GEN.21
5.4	**Production et conservation de traces**	
	Traçabilité des opérations effectuées au cours du cycle de vie des comptes, telles que la modification des attributs d'identité, la modification des autorisations, les tentatives de connexion, les tentatives de modification des mots de passe, etc.	SC.SSI/IAM.91

3.2.6 Autres fonctionnalités

Objectifs de production d'indicateurs pour le RIS en vague 2 :

Afin de suivre les usages en établissement de santé et d'obtenir des indicateurs pour le financement des programmes, la production de statistiques d'usage du DMP et de la MSSanté exploitables est essentielle.

Ces statistiques, se déclinent par site géographique (FINESS, SIRET et RPPS-Rang) suivant les structures à l'origine du partage des examens d'imagerie, par type de documents, par période temporelle, et concernent :

- L'alimentation des documents au DMP en direct ou via la fonction PFI ;
- La consultation et l'intégration des documents du DMP ;
- L'envoi des documents par MSSanté (professionnelle et citoyenne de Mon espace santé)
- L'intégration automatique des documents transmis par la MSSanté
- L'information et le consentement à la consultation et la non-opposition à l'alimentation de son DMP
- La qualification des INS des patients

Fonctionnalités couvertes par les exigences vague 2 :

Autres fonctionnalités - Fonctionnalités du périmètre Vague 2	Exigences associées
6.1 Production d'indicateurs	
Fourniture de statistiques	SC.STAT/ES.04 TBB.INS.03
6.2 Suivi des services ANS en temps réel	
Renvoie vers la météo des services ANS	SC.STATPP.01

Le système DOIT fournir les statistiques mensuelles :
• par site géographique (FINESS, SIRET, RPPS-Rang)
• par type de document (demande d'Acte d'Imagerie et Compte Rendu d'Imagerie)
• par période temporelle (à minima tous les mois de l'année courante et de l'année précédente)

Concernant notamment :

Statut des identités :

- Nombre et taux d'identités pour chaque statut (provisoire, récupéré, validé et qualifié)

Alimentation du DMP :

- Nombre d'alimentations de compte rendu d'imagerie transmis à la PFI, transmis au DMP (réussi, invisible au patient, en échec, pour lesquels le DMP du patient n'existe pas)

Consultation du DMP

- Nombre d'utilisateurs du RIS pouvant consulter le DMP, nombre d'utilisateurs radiologues ou médecins nucléaires, nombre d'utilisateurs manipulateur en électroradiologie, nombre d'utilisateurs autres

Information du patient à l'utilisation de son DMP :

- Total pour lesquels le consentement du patient à la consultation de son DMP a été enregistrée
- Total pour lesquels la non-opposition du patient sur l'alimentation de son DMP a été enregistrée

Envoi vers la MSSanté professionnelle et la MSS citoyenne de Mon espace Santé :

- Nombre de compte rendu d'imagerie médicale envoyés par MSSanté à des BAL MSSanté pro (réussi, en échec, non envoyé), Nombre de documents envoyés par MSSanté à des BAL MSSanté citoyennes (réussi, en échec, non envoyé).
- Nombre de documents CDA intégrés depuis la BAL APP par un utilisateur dans le RIS (réussi, en échec).

Ces statistiques doivent être disponibles via une interface dédiée et par une extraction de type csv (le format attendu est celui du fichier modelestat_IMG_RIS) - voir la page de présentation du dispositif RIS du Couloir Imagerie du Ségur du numérique en santé (lien : Le dispositif RIS du Couloir Imagerie du Ségur du numérique en santé | Portail Industriels)

3.2.7 Conformité aux autres services socles

L'appli carte Vitale (ApCV) est un portefeuille de cartes Vitale individuelles dématérialisées, chacune portant les données d'identification d'un seul bénéficiaire. Il s'agit d'un dispositif sécurisé d'authentification sur système mobile permettant l'accès aux services de l'assurance maladie.

Elle permet d'authentifier de manière simple et sécurisée les assurés, via leur smartphone. Elle leur permet également d'accéder à tous les services en ligne de santé proposés par le GIE Sesam-Vitale.

Dans le cas de la facturation SESAM-Vitale, l'utilisateur de l'ApCV est la personne qui présente son ApCV au Professionnel de Santé. L'authentification de cet utilisateur permet d'obtenir un contexte ApCV qui contient :

- Les données de la carte Vitale individuelle dématérialisée permettant d'identifier l'utilisateur de l'ApCV ;
- Éventuellement les données des cartes Vitale individuelles dématérialisées permettant d'identifier d'autres bénéficiaires ;
- Les informations relatives à l'ApCV.

La carte Vitale individuelle dématérialisée porte les données d'identification d'un seul bénéficiaire et de son organisme gestionnaire.

Autres fonctionnalités - Fonctionnalités du périmètre Vague 2	Exigences associées
7.1 Gestion de l'application carte vitale	
Gestion de l'application carte vitale	SC.APCV.01

3.2.8 Identité Nationale de Santé

Fonctionnalités couvertes par les exigences vague 2 :

N°	GESTION DE L'IDENTITE NATIONALE DE SANTE- Fonctionnalités du périmètre Vague 2	Exigences associées
8.1	**Gestion code officiel géographique (COG) du lieu de naissance**	
	Implémentation des référentiels de l'INSEE des codes officiels géographiques	SC.INS.01 SC.INS.02 SC.INS.03 SC.INS.05 SC.INS.06
8.2	**Gestion du statut des identités**	
	Intégration de l'INS qualifiée lorsqu'elle est récupérée à partir de l'Appli carte Vitale	SC.INS.04 SC.INS.22
8.3	**Production d'indicateurs**	
	Production d'indicateurs pour permettre un meilleur suivi	SC.INS.09 SC.INS.10 SC.INS.17
8.4	**Gestion de l'identité**	
	Vérification périodique de l'identité Interrogation du téléservice INSi à partir de la carte vitale, méthode à privilégier Faciliter la comparaison entre le retour du téléservice INSi et l'identité locale	SC.INS.13 SC.INS.14 SC.INS.15 SC.INS.19 SC.INS.22 SENTINELLE.02 SENTINELLE.05 SENTINELLE.07
8.5	**Gestion du contrat de confiance**	
	Permettre la transitivité de l'INS lorsqu'elle est transmise par un acteur extérieur de confiance	SC.INS.11 SC.INS.20
8.6	**Propagation de l'identité**	
	Intégration de l'INS à la Modality Worklist (MWL) SCP	RIS.INS/va2.02

L'utilisation de l'Identité Nationale de Santé (INS) pour référencer les données de santé est une obligation réglementaire depuis le 1er janvier 2021. L'Identité Nationale de Santé permet à tous les professionnels impliqués dans la prise en charge d'un patient de l'identifier de manière unique et pérenne. L'objectif est multiple : **réduire les risques d'erreur d'identité et améliorer la qualité des soins, permettre un accès immédiat aux données de santé d'un patient dès le début de sa prise en charge via Mon espace santé et**

fluidifier également le partage des documents de santé avec le patient et entre professionnels, que ce soit dans Mon espace santé ou via les messageries sécurisées de santé.

L'objectif national est de permettre à 90 % de la population de bénéficier d'une INS qualifiée. Pour atteindre cet objectif, il était crucial de prendre en compte les retours des professionnels de santé, ainsi que les observations faites lors des visites de référencement des logiciels dans le cadre du programme Ségur numérique. Ces retours ont souligné la nécessité d'améliorer l'ensemble du corpus documentaire INS, pour maximiser les chances de lier les données de santé des patients à leur INS et de compléter les exigences du guide d'implémentation éditeurs.

La vague 2 vise en particulier les objectifs métiers suivants :

- Intégrer l'Appli carte vitale : une avancée significative dans la procédure de qualification de l'INS. Grâce à l'Appli carte vitale, l'identité est récupérée directement au statut qualifié. Cette amélioration va faciliter le travail des utilisateurs finaux et ainsi simplifier et fluidifier la communication entre les professionnels de santé et les patients.
- Faciliter les processus et rendre l'INS plus accessible et plus facile à utiliser au quotidien.

Pour répondre à ces objectifs, et plus particulièrement dans le Guide d'implémentation, certaines exigences introduites lors de la vague 1 ont été reprises, d'autres ont été clarifiées afin d'apporter plus de précisions, tant du point de vue des éditeurs que des utilisateurs, pour une meilleure compréhension et mise en œuvre. De nouvelles exigences ont été ajoutées afin de couvrir des périmètres qui n'étaient pas pris en compte précédemment.

Rappel réglementaire : qualification de l'INS et échange / partage de données de santé

NB : Nous employons indifféremment "INS qualifiée" ou "identité au statut qualifié".

Pour rappel, tous les documents de santé doivent depuis janvier 2021 être référencés avec une INS.

Il est important de dissocier les deux types de flux d'alimentation : envoi au Dossier Médical Partagé (DMP) et envoi via la messagerie sécurisée de santé (MSSanté).

Ces 2 canaux répondent à des prérequis différents quant à la qualification de l'INS :

- La qualification de l'INS est obligatoire au versement dans le DMP / Mon espace santé
- La qualification de l'INS n'est pas obligatoire pour l'envoi des documents via la MSSanté

Bien qu'il soit fortement recommandé de transmettre des documents avec une INS qualifiée, il est possible de transmettre par MSSanté des documents sans INS qualifiée aux professionnels de santé, afin de sécuriser la transmission des informations nécessaires au suivi de son patient.

De même, pour qu'un professionnel puisse écrire à un patient (<MatriculeINS>@patient.mssante.fr), son INS doit en principe être qualifiée. Toutefois, une dérogation est intégrée dans le Référentiel #2 Client de Messagerie pour prendre en compte les cas d'usage de la préadmission et la réalité de la qualification de l'INS, cette dérogation restera valable jusqu'à révocation dans une future version du même référentiel.

Faciliter le référencement des données de santé avec l'identité nationale de santé (INS) dans les Logiciels pour éviter les erreurs d'identitovigilance.

Le code officiel géographique du lieu de naissance (COG)

Le COG est la principale cause de discordances entre l'INS et les traits présents sur le dispositif à haut niveau de confiance. Cela peut s'expliquer du fait qu'une commune a fusionné avec une autre. Afin de faciliter la mise en cohérence des traits INS et ceux présents dans la base locale, il est nécessaire de :

- Implémenter les différents référentiels de l'INSEE des COG avec leurs historiques pour les communes, pays, évènements sur les communes, communes depuis 1943, communes des collectivités d'outre-mer.

- Permettre à l'utilisateur d'accepter un code INSEE du téléservice lorsqu'il est absent dans le référentiel fourni par l'éditeur.
- Interroger le téléservice INSi « par saisie des traits d'identité » en 1ère intention sans le COG, afin de favoriser le retour d'une INS.
- Permettre lorsque le lieu de naissance est inconnu de saisir « INCONNU » avec le COG « 99999 » sans le préremplir par défaut lors de la création d'une identité

Favoriser la récupération de l'INS à partir du téléservice

La récupération de l'INS via la carte Vitale est la méthode privilégiée car elle facilite et sécurise l'obtention de l'INS correspondant à l'identité recherchée.

La Vague 2 rappelle l'importance de cette méthode et introduit l'Appli carte Vitale, qui simplifie davantage ce processus.

Il est essentiel de distinguer la récupération de l'INS via la carte Vitale, qui permet d'obtenir une identité au statut « récupéré », de l'utilisation de l'Appli carte Vitale. Cette dernière permet de récupérer et de qualifier de manière plus rapide et efficace. Une fois l'identité d'un patient récupérée via l'Appli carte Vitale, que ce soit par scan du QR code ou par lecture NFC, l'utilisateur peut considérer l'identité comme qualifiée. L'Appli carte Vitale permet ainsi de gagner du temps dans le processus de qualification et d'étendre l'accès à l'INS à un plus grand nombre d'usagers.

Pour rappel : gestion des statuts

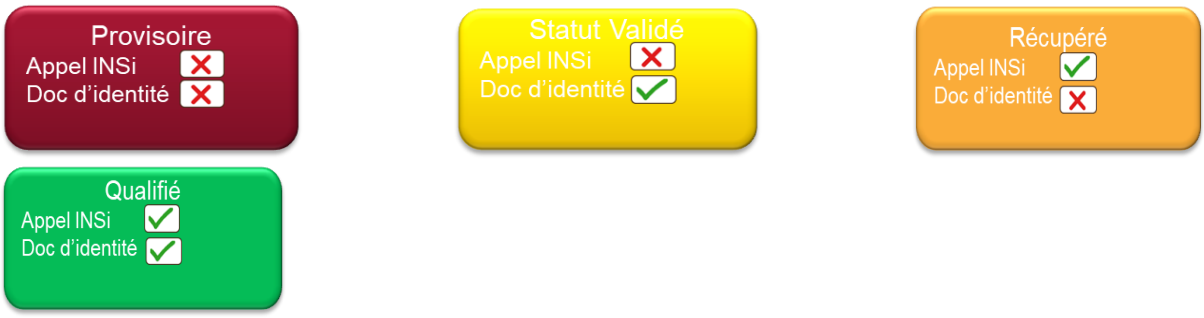
Conformément au Référentiel national d'identitovigilance (RNIV), l'enregistrement des traits d'identité doit être associé au niveau de confiance attribué à l'identité (statut de l'identité), en fonction des modalités de recueil et du contrôle de cohérence des informations.

Les statuts de l'identité sont :

- Identité provisoire
- Identité récupérée
- Identité validée
- Identité qualifiée

Pour faciliter la compréhension des utilisateurs, une info-bulle (fenêtre d'information affichée lors du survol de la souris du statut de l'identité pendant un temps > 1s) peut être ajoutée pour indiquer les actions à effectuer selon le statut de l'identité afin d'obtenir une identité qualifiée.

Par exemple :



Pour permettre aux professionnels de mieux identifier les identités nécessitant une attention particulière, il est possible d'utiliser des attributs tels qu'homonyme, douteux ou fictif en complément du statut de l'identité. Ces attributs offrent des indications supplémentaires pour un traitement spécifique, assurant ainsi une gestion plus précise et adaptée des cas complexes.

Permettre aux professionnels de bénéficier sous conditions de l'INS transmise par un tiers de confiance

La réception d'une donnée de santé avec une identité offre l'opportunité de faire évoluer le statut de l'identité locale, comme s'il s'agissait d'une venue de patient ou créer une identité lors de la réception de données de santé.

Toutefois, elle doit être accompagnée de garanties pour le récepteur de l'identité, afin d'éviter tout risque de collision et de propagation d'une INS attribuée à un mauvais patient. Ces garanties sont formalisées dans un contrat de confiance établi entre l'émetteur et le récepteur des données de santé.

La "clause ou contrat de confiance" est un engagement explicite et réciproque entre les différentes parties prenantes (utilisateurs, responsables de traitement, sous-traitants), garantissant le respect des bonnes pratiques en matière d'identitovigilance, conformément à la section correspondante du RNIV.

Ce contrat de confiance ne peut être établi que si l'émetteur de la donnée s'engage à réaliser un contrôle de cohérence via un dispositif d'identification de haut niveau de confiance.

Cette clause peut figurer :

- Dans un contrat de sous-traitance ;
- Dans une convention ou dans les conditions générales et/ou particulières d'utilisation (CGU) d'une application tierce (régionale ou autre).

Le contrat de confiance ne peut être appliqué que dans les cas suivants :

- Lorsqu'une structure prestataire de services n'est pas en mesure de vérifier l'identité du patient (patient jamais vu, par exemple : laboratoire de biologie secondaire, téléexpertise, téléradiologie
- Dans le cadre d'une admission partagée (exemple : un département de radiologie libéral associé à une clinique).

Lorsque ce contrat de confiance est en place, le récepteur de l'identité doit, s'assurer qu'entre la qualification de l'identité par l'émetteur et sa réception, l'identité n'a pas évolué et limiter tout risque d'ambiguïté. C'est pourquoi il doit procéder à l'opération de récupération à partir des traits reçus par flux, en appelant le téléservice INSi pour toute identité reçue, si l'identité n'est pas déjà présente dans la base locale au statut récupéré ou qualifié.

Lorsque le téléservice INSi renvoie : une identité trouvée (retour 00), la validation de l'identitovigilance ayant été acquise via le contrat de confiance, alors le système peut intégrer l'identité directement au statut qualifié, si elle était qualifiée par l'émetteur. Dans le cas contraire, le système doit permettre à l'utilisateur de créer une nouvelle identité avec le statut précisé dans la matrice ci-dessous.

Lors de la réception par flux informatique pour d'une identité avec le statut d'identité validée ou qualifiée, si le type de dispositif de haut niveau de confiance utilisé n'est pas précisé, la mention "tiers de confiance" doit être sélectionnée. Le système doit ajouter « tiers de confiance » dans la liste des dispositifs à haut niveau de confiance

La matrice ci-dessous précise le statut final de l'identité dans le SI local après intégration de l'identité reçue, dans le cadre d'un contrat de confiance entre les deux entités.

Un mécanisme de rapprochement entre une éventuelle identité préexistante dans le SI local et l'identité reçue est systématiquement mis en œuvre (calcul d'un taux de ressemblance ou décision humaine). Si le receveur n'est pas en mesure de s'assurer que l'identité transmise et celle préalablement existante dans le SI local correspondent au même usager, une nouvelle identité doit être créée.

A noter : Le calcul du taux de ressemblance entre une identité locale et une identité reçue par flux informatique doit impérativement se baser sur les traits de l'INS (y compris matricule INS) lorsque l'identité est qualifiée des deux côtés. Si ce n'est pas le cas, le calcul doit inclure l'ensemble des traits stricts ainsi que des informations complémentaires comme le numéro de sécurité sociale.

		Statut de l'identité dans le SI local							
		IDENTITE NON CONNUE		**RECUPERE**		**VALIDE**		**QUALIFIE**	
	Retour de récupération INSi appelé avec traits reçus hors COG	1 identité trouvée (00)	Aucune (01) ou plusieurs identités trouvées (02)	1 identité trouvée (00)	Aucune (01) ou plusieurs identités trouvées (02)	1 identité trouvée (00)	Aucune (01) ou plusieurs identités trouvées (02)	1 identité trouvée (00)	Aucune (01) ou plusieurs identités trouvées (02)
	Action à réaliser	Proposer de créer une nouvelle identité avec traits reçus	Proposer de créer une nouvelle identité avec traits reçus	Rapprocher les identités	Proposer de créer une nouvelle identité avec traits reçus	Proposer de créer une nouvelle identité avec traits reçus	Proposer de créer une nouvelle identité avec traits reçus	Rapprocher les identités	Proposer de créer une nouvelle identité avec traits reçus
Statut de l'identité reçue	**VALIDE**	Qualifié	Validé	Qualifié	Validé	Qualifié	Validé	Qualifié	Validé
	QUALIFIE	Qualifié	Validé	Qualifié **(Pas d'appel au TLSi)** rapprochement des identités		Qualifié	Validé	Qualifié **(Pas d'appel au TLSi)** rapprochement des identités	

Lorsque l'identité transmise est au statut provisoire et qu'une identité existe dans le SI local, une nouvelle identité doit être créée au statut provisoire.

		Statut de l'identité dans le SI local				
		IDENTITE NON CONNUE	**PROVISOIRE**	**RECUPERE**	**VALIDE**	**QUALIFIE**
		Créer une nouvelle identité avec traits reçus	Créer une nouvelle identité avec traits reçus	Créer une nouvelle identité avec traits reçus	Créer une nouvelle identité avec traits reçus	Créer une nouvelle identité avec traits reçus
Statut de l'identité reçue	**PROVISOIRE**	Provisoire	Provisoire	Provisoire	Provisoire	Provisoire

Lorsqu'un contrat de confiance est en place avec un tiers, le système doit permettre à l'utilisateur de spécifier avec quel(s) correspondant(s) ce contrat est établi, via une table de paramétrage.

Lorsque le demandeur est inconnu du récepteur ou que la qualité de ses pratiques d'identitovigilance n'est pas garantie par un contrat, les mécanismes de transitivité de l'identité mentionnés précédemment ne peuvent pas être appliqués.

En l'absence de contrat de confiance, l'identité reçue ne peut être créée qu'avec le statut « identité provisoire », à moins qu'elle ne soit déjà présente dans le système d'information du récepteur avec un statut plus élevé, ou au statut récupéré si une opération d'appel au téléservice INSi est réalisé dans le système local et retrouve une identité 00.

Faciliter aux utilisateurs la gestion de l'identité et le processus de qualification de l'identité

Si l'identité de l'usager n'est pas déjà qualifiée ou récupérée, le système doit automatiquement interroger le téléservice INSi lors de l'insertion de la carte Vitale ou à l'ouverture du dossier, en utilisant en priorité les données de la carte Vitale ou, à défaut, les traits d'identité.

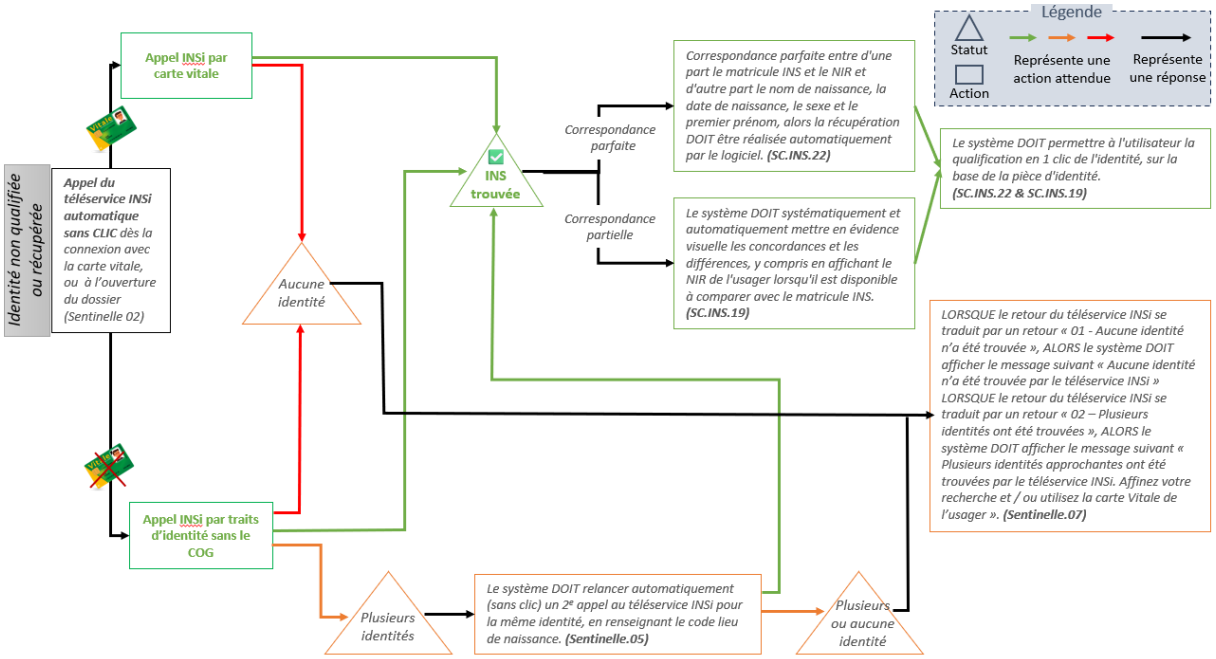
En cas de retour unique du téléservice INSi, les concordances et divergences entre les données sont mises en évidence visuellement, permettant à l'utilisateur de valider l'identité en un clic.

Si toutes les informations concordent parfaitement (matricule INS, NIR, nom de naissance, 1er prénom de naissance, date de naissance, sexe), la récupération de l'identité se fait automatiquement. Si l'identité n'est pas encore validée, l'utilisateur peut la qualifier rapidement à partir de la pièce d'identité.

Lorsque le système tente de récupérer une identité via le téléservice INSi sans code lieu de naissance et obtient un retour « 02 – Plusieurs identités ont été trouvées », il doit automatiquement relancer l'appel avec le code lieu de naissance sans informer l'utilisateur. Si la relance aboutit à une identité unique (« 00 »), le système met en évidence visuellement les concordances et différences, notamment le NIR, permettant ensuite à l'utilisateur de valider l'identité en un clic.

En cas de retour du téléservice INSi « 01 – Aucune identité trouvée » ou « 02 – Plusieurs identités trouvées », le système affiche un message adapté et propose des conseils ou un lien explicatif pour aider l'utilisateur à affiner la recherche ou utiliser la carte Vitale.

Le schéma ci-dessous décrit précisément le mécanisme à mettre en place.



Appel à l'opération de vérification

Le système doit automatiser plusieurs processus pour périodiquement actualiser, les identités au moyen de l'opération de vérification du téléservice INSi lorsque :

- L'identité a été récupérée où qualifiée depuis 4 ans,
- Le matricule INS est de type NIA, à l'occasion d'un nouvel événement.

Si la vérification échoue, une opération de récupération est lancée en utilisant les informations locales.

3.2.9 Exigences issues de la vague 1 RIS

Le périmètre « Vague 1 » est issu de la vague 1 du Ségur numérique pour les RIS, qui visait en particulier à systématiser l'alimentation du profil Mon espace santé du patient à chaque épisode de soins. Pour les RIS, ces exigences vague 1 concernaient notamment :

- La génération de certains types de documents en particulier la lettre de liaison de sortie, les ordonnances de sortie et le compte-rendu opératoire ;
- L'envoi de ces documents et données numériques par MSSanté vers un professionnel de santé ou vers le patient, et leur alimentation dans le DMP du patient ;
- La conformité aux référentiels et services socles du numérique en santé (INS, Pro Santé Connect) ;
- La conformité INS avec la prise en charge de l'Identité Nationale de Santé (INS) dans les standards d'interopérabilité et les volets du CI-SIS.

Certaines exigences initialement présentes dans le dispositif vague 1 ne sont pas reprises à l'occasion de la vague 2, car rendues « obsolètes » par des exigences du périmètre « Vague 2 » couvrant les mêmes fonctionnalités, et bénéficiant des retours terrain du déploiement de la vague 1.

Sous réserve des dispositions de la section 3.1.3, le dépôt des preuves correspondant à ce périmètre « Vague 1 » **n'est pas exigé pour les solutions déjà référencées dans la cadre de la vague 1.**

Fonctionnalités du périmètre « Vague 1 » :

CHAPITRE	FONCTIONS VA1	EXIGENCES ASSOCIÉES
Gestion de l'Identité Nationale de Santé	Conformité INS et gestion du téléservice INSi	INS/va1.01 à INS/va1.12 INS/va1.15 INS/va1.18 INS/va1.20 à INS/va1.23 INS/va1.25 à INS/va1.27 INS/va1.31 à INS/va1.33 INS/va1.35 INS/va1.36 INS/va1.41 INS/va1.44 INS/va1.46 à INS/va1.52 INS/va1.54 à INS/va1.60 INS/va1.68 INS/va1.69
	Appel Contextuel avec l'INS	AC/va1.01
Consultation et Alimentation du DMP / Mon espace santé	Modification et suppression	DMP/va1.09
	Génération des métadonnées XDS pour l'envoi au DMP du CR d'Imagerie	DMP/va1.10
	Consultation du webPS DMP par appel contextuel	DMP/va1.11
	Blocage de l'alimentation	DMP/va1.12
	Alimentation systématique de Mon espace santé	DMP/va1.13
	Paramétrage des données de masquage et de l'opposition à l'envoi au DMP	DMP/va1.14
	Gestion des certificats RPPS-rang	AUTH/va1.01
Gestion de la MSSanté	Envoi sécurisé vers la messagerie de Mon espace santé d'un patient	MSS/va1.01 MSS/va1.17
	Envoi de messages et de documents CDA R2 par MSSanté	MSS/va1.02 MSS/va1.04

		MSS/va1.08 MSS/va1.09 MSS/va1.11 MSS/va1.12 MSS/va1.14 MSS/va1.15 MSS/va1.16 MSS/va1.20 MSS/va1.21 MSS/va1.29 MSS/va1.30 MSS/va1.40
	Intégration de l'annuaire santé	ANN/va1.01 à ANN/va1.05
Gestion et partage des documents de santé	Production des documents au format CDA R2 conformes au CI-SIS	DOC/va1.01 DOC/va1.04 DOC/va1.05 DOC/va1.15 DOC/va1.17
	Gestion des CR d'imagerie	CRI/va1.01 à CRI/va1.07
Autres fonctionnalités	Portabilité des données	PORT/va1.01

4. MODALITES DE REFERENCEMENT DE LA SOLUTION LOGICIELLE

4.1. Principes de référencement de la Solution logicielle

Le référencement Ségur vague 2 est attribué à toute Solution logicielle respectant le périmètre décrit à la Section 2, et faisant la preuve du respect des Exigences du Référentiel d'Exigences Minimales (REM).

Solution logicielle candidate au référencement

Dans le cas où l'Editeur commercialise plusieurs Solutions logicielles couvrant le périmètre fonctionnel du DSR-IMG-RIS-Va2, il peut solliciter des référencements pour chacune de ces Solutions logicielles en déposant autant de candidatures que de Solutions logicielles à référencer.

La demande de référencement se fait pour une Version candidate d'une Solution logicielle. Le référencement précise le ou les Profils pour lesquels la Solution Candidate a satisfait aux Exigences.

Note sur l'identification des versions logicielles et numérotations :

- *Le Numéro de version technique est aisément accessible à l'utilisateur dans l'IHM (Interface Homme-Machine) de la Solution logicielle.*
- *La succession chronologique des Versions techniques doit être clairement compréhensible au travers d'une numérotation alphanumérique.*

Contrôles du respect des Exigences

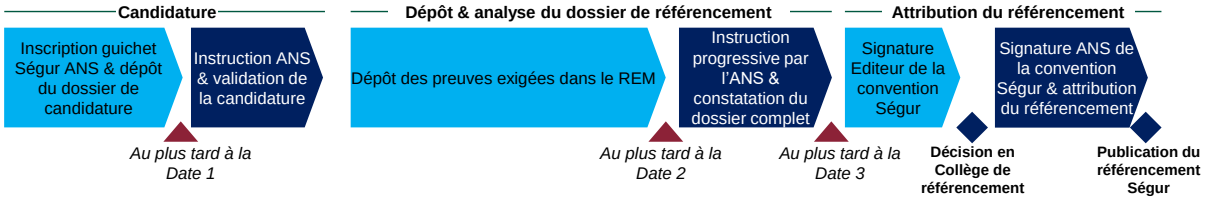
Les preuves de conformité aux Exigences déposées par l'Editeur font l'objet de contrôles effectués lors de la phase d'instruction du dossier par les équipes de l'ANS et conformément aux scenarii de vérification de conformité détaillés dans le REM-IMG-RIS-Va2.

L'Editeur fournit à l'ANS en toute circonstance des informations exactes et reflétant fidèlement les caractéristiques et fonctionnalités de la Solution logicielle.

Parcours de référencement

Le parcours de référencement Ségur de la Solution logicielle se déroule auprès de l'ANS via la plateforme en ligne Convergence, en 3 grandes phases :

- Le dépôt et la validation du dossier administratif
- Le dépôt des preuves de conformité et l'instruction par l'ANS
- L'attribution du référencement



L'accès à la plateforme Convergence et aux autres services Ségur de l'ANS se fait depuis l'Espace Authentifié [1], qui nécessite l'enregistrement préalable au fournisseur d'identité « Industriels Santé Connect » (iSC[2]). Depuis la page d'accueil du Portail Industriels :

[1] Voir les CGU disponibles sur https://industriels.esante.gouv.fr/cgu-portail-industriels
[2] Voir les CGU disponibles sur https://isconnect.esante.gouv.fr/enrollement/account/cgu

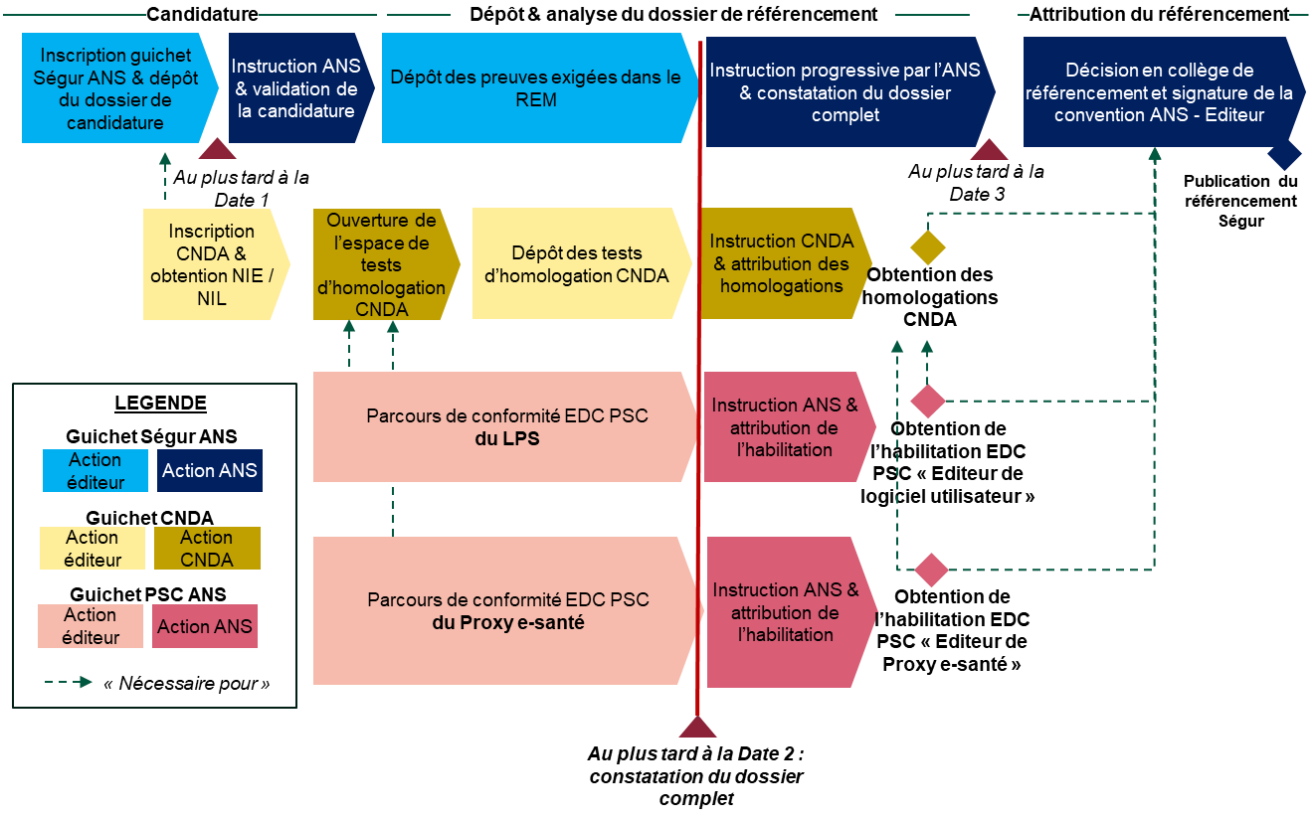
- **S'enregistrer** au fournisseur d'identité iSC en fournissant les documents justificatifs nécessaires à la vérification de l'identité de l'entreprise (Kbis, pièce d'identité du mandataire).
- **Se connecter** à l'Espace Authentifié une fois l'inscription à iSC validée.

Articulation avec les démarches à réaliser auprès du CNDA et du Guichet Pro Santé Connect de l'ANS

Dans le cadre de son parcours de référencement Ségur vague 2, l'Editeur doit obtenir pour sa Solution logicielle candidate au référencement Ségur :

- **Auprès du guichet Espace de confiance Pro Santé Connect de l'ANS (EDC PSC), l'habilitation « Editeur de logiciel utilisateur »** , selon les dispositions du référentiel PSC, et qui implique notamment :
  - La complétion des chapitres d'exigences de l'espace de dépôt de preuves de ce quichet, correspondant aux exigences présentées dans le document de confomité (N1) ;
  - Le raccordement réussi au bac à sable PSC (N2) ;
  - Et la réalisation d'un test d'intrusion (N4) auprès d'un auditeur qualifié PASSI, attestant d'un niveau de conformité suffisant.
- **Auprès du guichet Espace de confiance Pro Santé Connect de l'ANS (EDC PSC), l'habilitation « Editeur de Proxy e-santé »**, selon les dispositions du référentiel PSC, ce qui implique notamment :
  - La complétion des chapitres d'exigences de l'espace de dépôt de preuves de ce quichet, correspondant aux exigences présentées dans le document de confomité (N1) ;
  - Le raccordement réussi au bac à sable PSC (N2) ;
  - La validation des tests à l'aide de l'outil de conformité ANS (N3)
  - Et la réalisation d'un test d'intrusion spécifique au composant Proxy e-santé (N4) auprès d'un auditeur qualifié PASSI, attestant d'un niveau de conformité suffisant.
- **Auprès du CNDA, les homologations exigées dans le REM, en tenant compte des éléments suivants :**
  - Si la Solution logicielle ne dispose pas déjà d'un référencement Ségur vague 1 de l'ANS, les identifiants du dossier CNDA (numéro d'identification éditeur NIE et numéro d'identification logiciel NIL) sont nécessaires pour compléter le dossier de candidature Ségur ;
  - La réalisation des tests d'homologation auprès du CNDA nécessite l'utilisation par la Solution logicielle d'un **composant Proxy e-santé. Le démarrage de ces tests d'homologation est conditionné à l'atteinte d'un niveau de maturité suffisant de la Solution logicielle et du composant Proxy e-santé dans leurs parcours d'habilitation PSC, définis par l'ANS ;**
  - La décision finale d'homologation du CNDA nécessite d'avoir obtenu au préalable les habilitations EDC de la Solution logicielle et du composant Proxy e-santé (habilitations dites « Editeur de logiciel utilisateur » et « Editeur de proxy e-santé »)

Au global, le parcours complet de référencement s'organise de la façon suivante :



NB : les notions « Date 1 », « Date 2 » et « Date 3 » sont définies à la Section 4.2, et les règles de gestion associées sont explicitées aux Sections 4.3 et 4.4.

Audits de conformité post-référencement

Des audits de conformité peuvent être réalisés par l'ANS après l'obtention du référencement Ségur. Ils ont pour objet de contrôler la conformité aux Exigences du référencement de la Solution logicielle telle qu'elle est effectivement commercialisée ainsi que le caractère opérationnel de ses fonctionnalités. Ils sont réalisés majoritairement *in situ* chez un utilisateur de la Solution logicielle, et comprennent également les contrôles de conformité vis-à-vis des différentes obligations contractuelles.

L'Editeur s'engage à se soumettre à tout audit de conformité de la Solution logicielle ainsi qu'à y apporter leur concours, conformément aux instructions qui leur seront données.

Les modalités des audits de conformité et les conséquences en découlant sont définies dans la convention de référencement.

Publicité des informations

L'ANS publie sur son site Internet les principales informations décrivant la liste des candidats (couple Editeur-Solution) en cours de référencement pour chaque dispositif de la vague 2. Elle y inclut également les détails relatifs aux Solutions logicielles ayant obtenu leur référencement, en fournissant l'ensemble des informations nécessaires aux Clients pour garantir la conformité avec les dispositions du SONS.

4.2. Calendrier du SONS IMG-RIS-Va2

Le système ouvert et non sélectif (SONS) pour IMG-RIS-Va2 est mis en œuvre selon le calendrier suivant :

Date de parution au JO de l'arrêté ministériel relatif à la vague 2, ci-après **Date 0**	Lancement du SONS IMG-RIS-Va2
Mercredi 10 septembre 2025 12h, ci-après **Date 1**	**REFERENCEMENT** : Date limite de dépôt du dossier administratif à l'ANS
Mercredi 13 mai 2026 12h, ci-après **Date 2**	**REFERENCEMENT** : Date limite de dépôt d'un dossier complet de preuves de conformité
Mercredi 16 septembre 2026 12h, ci-après **Date 3**	**REFERENCEMENT** : Date de fin des échanges entre l'Editeur et l'ANS pour validation du dossier de preuves
Mardi 10 novembre 2026 12h, ci-après **Date 4**	**FINANCEMENT** : Fin de la période de réception des demandes de financement et de versement de l'avance. Toute demande de financement et de versement d'une avance postérieure à cette date est irrecevable.
Mercredi 9 juin 2027 12h, ci-après **Date 5**	**FINANCEMENT** : Fin de la période de réalisation des Prestations principales par les Fournisseurs. A cette date, le Fournisseur doit, soit avoir déposé sa demande de solde, soit avoir envoyé son attestation de fin de Prestation principale, selon les modalités présentées à la Section 6.4 de l'AF-IMG-RIS-Va2.
Mercredi 22 septembre 2027 12h, ci-après **Date 6**	**FINANCEMENT** : Fin de la période de réception des demandes de paiement du solde de la Prestation principale. Toute demande de paiement du solde postérieure à cette date est irrecevable.

Toute demande, de quelque nature qu'elle soit, liée à la mise en œuvre du SONS est réputée effectuée à la date à laquelle elle a été reçue par l'ANS ou l'ASP, selon les cas.

4.3. Phase 1 - Dépôt et validation du dossier administratif

Le dossier administratif est composé d'une candidature administrative et d'un formulaire d'éligibilité.

La personne physique ou morale ayant le pouvoir d'engager la responsabilité de l'Editeur accepte d'appliquer les dispositons de la Charte de référencement Ségur qui décrit le déroulement des étapes clés de la démarche de référencement ainsi que les droits et devoirs de chaque partie prenante (Editeur et ANS).

L'acceptation de la Charte de référencement permet à l'Editeur d'accéder à l'espace de dépôt du dossier administratif sur la plateforme Convergence.

La date de dépôt du dossier administratif est la date à laquelle la candidature administrative et le formulaire d'éligibilité ont été soumis au moins une fois par l'Editeur. Cette date ne peut être postérieure à la **Date 1.**

L'ANS peut solliciter l'Editeur par l'intermédiaire de la plateforme Convergence pour toute demande de complément. Si l'Editeur ne répond pas à la sollicitation dans un délai de 5 jours ouvrés à compter de celle-ci, l'ANS se réserve le droit de rejeter sa demande de référencement, conformément aux dispositions inscrites dans la Charte de Référencement.

L'Editeur doit renseigner les informations indiquées ci-après pour chaque Version candidate qu'il inscrit dans le processus de référencement (les informations demandées qui sont signalées par une * sont obligatoires) :

Informations relatives à l'Editeur :

- Dénomination sociale de l'entreprise (*)
- Numéro d'identification SIRET de l'entreprise (*)
- Forme juridique de l'entreprise : SAS, Sarl etc. (*)
- Fonction du dirigeant / responsable légal de l'entreprise : CEO, Président, DG etc. (*)
- Adresse du siège social (*)
- Nom/Prénom du représentant légal de l'entreprise (*)
- Coordonnées e-mail et téléphoniques du représentant légal (*)
- Nom/Prénom de la personne à contacter dans le cadre du référencement (*)
- Coordonnées e-mail et téléphoniques de la personne à contacter (*)

Informations relatives à la Version candidate :

- Dénomination commerciale (*)
- Date prévisionnelle du dépôt de dossier de preuves complet
- Si référencée vague 1 :
    - Le numéro unique de référencement vague 1 (cf. dispositif RAD-RIS-Va1)
- La description de l'éventuel groupement d'Editeurs présentant la candidature au référencement, et le cas échéant, le(s) mandat(s) communiqué(s) par les membres du groupement au Chef de file. Dans le cas d'une demande de référencement présentée par un groupement de personnes non doté de la personnalité morale (groupement solidaire), les règles suivantes doivent être respectées :
- Une candidature unique au référencement est portée pour le groupement ;
- Le **Chef de file** du groupement est l'interlocuteur unique de l'ANS pendant tout le processus de référencement. Il représente le groupement pour toute démarche ou acte au titre du référencement de la Solution logicielle.

Informations CNDA[3] :

- Numéro d'Identification Editeur (NIE délivré par le CNDA) (*)
- Numéro d'Identification Logiciel (NIL délivré par le CNDA) (*)

Informations sur la Solution logicielle :

- Numéro de version technique soumise au référencement (*)
- Numéro unique de candidature au guichet espace de confiance Pro Santé Connect
- L'Editeur transmet à l'ANS les éléments suivants pour la version candidate :
    - N° de version technique ;
    - Nom de version commerciale (plusieurs versions techniques pouvant être rattachées à un nom de version commerciale ;
    - L'information si la version technique est référencée en vague 1.
- Pour les Solutions logicielles pour lesquelles l'Editeur entend mobiliser des financements Ségur au titre de l'AF-IMG-RIS-Va2, l'Editeur déclare la liste des versions techniques de la Solution logicielle ayant fait l'objet d'une information publique par l'Editeur auprès de ses Clients au plus tard à la **Date 0**, d'arrêt de maintenance ou d'arrêt de commercialisation. Ces versions sont concernées par les dispositions décrites à la Section 4.3 de l'AF-IMG-RIS-Va2.
- L'information si la Solution logicielle est commercialisée *via* des distributeurs mandatés et le cas échéant, la liste des Distributeurs ayant vocation à démarcher des Clients et faire des bons de commande de Prestations Ségur en leur nom propre, et donc à ce titre amenés à demander des financements auprès de l'ASP dans le cadre du présent dispositif : dénomination sociale, SIRET, date de signature du mandat de distribution, date de fin du mandat de distribution.

[3] L'industriel obtient les numéros NIE et NIL dès son inscription auprès du CNDA. Une solution référencée vague 1 dispose déjà de ces numéros.

La Documentation logicielle (*) :

- Documentation fournie par l'Editeur, précisant en quoi sa Solution logicielle répond aux critères de définition des fonctionnalités minimales décrites dans la Section 2 du présent DSR.

Profils pour lesquels l'Editeur demande le référencement de sa solution (*) :

- Le Profil général est sélectionné par défaut sur la plateforme Convergence car il est obligatoire pour tous les candidats.
- Les Profils optionnels sélectionnés seront modifiables en fonction des temporalités suivantes :
  - Jusqu'à la **Date 2**, il est possible d'en ajouter ;
- Tout au long du processus, il est possible d'en retirer.

Composant Proxy e-santé : le Fournisseur doit déclarer les éléments relatifs au Composant Proxy e-santé partie de la Solution logicielle

Composants additionnels (*) : le Fournisseur doit déclarer tous les composants additionnels de sa solution, en précisant pour chacun :

- Nom de l'Editeur du Composant additionnel ;
- Dénomination commerciale du Composant additionnel ;
- Version du Composant additionnel ;
- NIL du Composant additionnel, applicable uniquement s'il se substitue au Composant principal pour l'obtention d'une homologation CNDA ;
- Chapitre du REM concerné (liste déroulante).

4.4. Phase 2 - Dépôt de dossier complet de preuves de conformité & instruction par l'ANS

L'Editeur dépose la totalité des preuves de conformité attendues sur la plateforme Convergence.

La date de dépôt du dossier complet de preuves de conformité est la date à laquelle le formulaire de dépôt de preuves doit avoir été soumis avec des preuves répondant aux Exigences du REM-IMG-RIS-Va2, déposées au moins une première fois par l'Editeur. Cette date ne peut être postérieure à la **Date 2**.

Un dossier complet de preuves de conformité correspond à un dossier dont l'Editeur a fourni :

- L'ensemble des preuves attendues, en tenant compte des dispositions de la Section 3.1. Pour chaque Exigence, les preuves de conformité à fournir sont décrites dans le REM. Plusieurs preuves de conformité peuvent être demandées pour attester de la conformité de la Solution logicielle à une même Exigence (capture d'écrans, vidéos, fichiers, logs, homologations…).
  - Le dépôt des preuves peut être effectué par chapitre sur la plateforme Convergence.
  - Chaque preuve demandée sur la plateforme Convergence est obligatoire.

- Pour chaque homologation à obtenir auprès du CNDA : l'attestation d'homologation, ou à défaut un compte-rendu **de pré-examen** du dossier d'obtention de l'homologation concernée (compte-rendu de pré-examen déclenchant une date d'examen via une copie d'écran de son espace personnel CNDA) ;

- Pour l'habilitation EDC PSC Editeur de logiciel utilisateur, le dossier complet des éléments attendus, tels que décrits dans le référentiel Pro Santé Connect.

- Pour l'habilitation EDC PSC Editeur de Proxy e-santé, le dossier complet des éléments attendus, tels que décrits dans le référentiel Pro Santé Connect.

  NB : L'obtention des habilitations EDC PSC pour les rôles Editeur de logiciel utilisateur et Editeur de Proxy e-santé impliquent la validation du rapport de test d'intrusion du rôle concerné. Il est de la responsabilité de l'éditeur de juger de l'opportunité de procéder, si nécessaire à de nouveaux tests d'intrusion en cas d'écart significatif entre la version du logiciel ayant obtenu l'habilitation PSC considérée et la dernière version présentée pour le référencement Ségur. Toute nouvelle version de rapport de test d'intrusion sera à transmettre à l'ANS.

L'ANS instruit l'analyse des preuves de conformité reçues et peut, le cas échéant, solliciter l'Editeur en cas de preuves non conformes.

Règles de traitement des dossiers et délais :

L'instruction s'effectue suivant une file d'attente déterminée par l'ordre de réception d'un chapitre complet de dépôt de preuves de conformité.

Pendant l'instruction du dossier, une phase d'échanges entre l'ANS et l'Editeur peut être nécessaire afin d'apporter des précisions sur les éléments de preuves fournis par l'Editeur. Dans ce cas, l'ANS peut être amenée à solliciter l'Editeur via la plateforme Convergence.

Conformément à la Charte de référencement, lorsque l'Editeur est sollicité par l'ANS :

- La place dans la file d'attente est garantie dans le cas où l'Editeur répond dans les 24h après notification de la demande de complément par l'ANS.
- La demande de référencement est considérée comme abandonnée en cas d'absence de réponse de l'Editeur dans les 30 jours après la sollicitation de l'ANS.

La date limite de fin des échanges de l'Editeur avec l'ANS pour la validation du dossier de preuves de conformité est la **Date 3**, date à laquelle le formulaire de dépôt de preuve n'est plus ouvert. Au-delà de la **Date 3**, aucun nouvel échange entre l'Editeur et l'ANS ne peut intervenir et aucune réponse complémentaire de l'Editeur ne sera instruite.

Les Editeurs restant dans l'attente d'une attestation d'homologation de la part du CNDA, peuvent, à titre dérogatoire de la condition définie précédemment relative à la **Date 3,** transmettre à l'ANS les éléments justificatifs (compte-rendu de pré-examen déclenchant une date d'examen via une copie d'écran de son espace personnel CNDA) au-delà de cette date limite.

Dans la même logique, si la décision d'habilitation Editeur de logiciel utilisateur ou de l'habilitation Editeur de Proxy e-santé de l'EDC PSC intervient après la **Date 3** du fait de l'ANS, celle-ci pourra être intégrée au dossier de référencement.

4.5. Phase 3 - Signature de la convention Ségur par l'Editeur et attribution du référencement

Sur la base du dossier complet, et une fois l'ensemble des preuves validées, l'ANS prépare le projet de convention de référencement Ségur et le soumet à l'Editeur pour signature électronique ; l'Editeur signe ensuite le projet de convention de référencement.

La convention de référencement, décrit l'ensemble des droits et devoirs à respecter dans la durée, par l'Editeur et par l'ANS, dans le cadre du référencement. Le convention précise notamment la durée du référencement (art.5). Une convention d'un référencement obtenu dans le cadre de la vague 1 du Ségur reste en vigueur à la suite d'un référencement obtenu en vague 2.

La signature de la convention par l'Editeur est un prérequis pour la présentation du dossier au collège technique de référencement. Lors du collège technique de référencement, le dossier candidat est examiné par les membres du collège qui lui attribuent ou non le référencement Ségur.

Collège technique de référencement

Après la phase d'instruction du dossier, un collège technique de référencement décide de l'attribution ou du refus du référencement de la Solution logicielle. Ce collège se tient de manière hebdomadaire et est composé de membres de l'ANS participant à l'instruction du dossier de candidature, et éventuellement de ses partenaires (CNDA/GIE SV/CNAM).

Le collège peut statuer de deux manières sur la Solution logicielle candidate :

- **Attribution du référencement** : la version technique de la Solution logicielle candidate au référencement est référencée en l'état ;
- **Réserves bloquantes : non attribution du référencement.** La décision de non-attribution du référencement est communiquée à l'Editeur ainsi que la ou les raisons expliquant cette décision. Dans le cas où cette décision intervient avant la Date 3, l'Editeur peut redéposer les preuves considérées non-conformes.

Notification de l'Editeur

A la suite de la tenue du collège technique de référencement, l'Editeur est notifié de la décision de l'ANS via la plateforme Convergence, ainsi que par courriel.

L'Editeur de la Solution logicielle référencée (ou le Chef de file en cas de groupement d'Editeurs) reçoit une attestation de référencement ANS.

Utilisation du Logo de référencement Ségur

Dès lors qu'une Solution logicielle est déclarée référencée l'Editeur peut utiliser le logo de référencement Ségur de l'ANS. Le logo ne peut être utilisé que pendant la durée de la présente Convention et exclusivement pour les finalités et le périmètre de celle-ci. L'Editeur ne peut utiliser le logo qu'à compter de la signature de la présente Convention par les deux parties (Editeur et ANS).

L'Editeur s'engage à ne pas utiliser le logo en violation des dispositions des présentes, ainsi qu'à des fins ou dans des conditions illicites, contraires à l'ordre public ou aux bonnes mœurs, susceptibles de porter atteinte aux droits ainsi qu'à l'image de l'ANS ou de tout tiers.

En cas d'usage abusif du logo "Référencé Ségur", l'Agence du numérique en santé appréciera l'opportunité d'engager les démarches décrites dans la Convention (pour mémoire et à toutes fins utiles cf. art. 12 à 18 de la convention de référencement).

4.6. Espace Authentifié, Support et FAQ

Utilisation des services proposés par l'Espace Authentifié

Une fois authentifié, l'Editeur peut, selon son Profil :

- Contacter son référent ANS : un gestionnaire de compte dédié, expert dans son domaine, pour accompagner l'Editeur dans ses démarches et le conseiller ;
- Consulter des notifications personnalisées en fonction de ses besoins, pour être au courant des dernières actualités, webinaires et évènements sur ses sujets de prédilection ;
- Consulter l'historique de ses demandes auprès de l'équipe accompagnement des Industriels de l'ANS et suivre l'avancement du traitement de ses demandes ;
- Consulter son tableau de synthèse de ses produits, préalablement enregistrés sur la plateforme Convergence, avec un accès direct pour consulter le détail de chacun d'entre eux ;
- Profiter d'un accès simplifié pour gérer son raccordement à Pro Santé Connect, sur les environnements de production et bac à sable ;
- Profiter d'un accès dédié pour activer l'API Sesali ;
- Gérer son Profil et modifier ses données et ses besoins.

L'Espace Authentifié propose un accompagnement sur-mesure, notamment dans le cadre du référencement Ségur et de nouveaux services continueront à être déployés pour informer, guider et orienter les éditeurs. Les candidats sont ainsi invités à activer leur Espace Authentifié pour bénéficier de fonctionnalités clés et trouver facilement les informations utiles dans le cadre de leur mise en conformité et stratégie réglementaire.

FAQ et Contact

Les candidats sont encouragés à se référer à la base de connaissances (FAQ des industriels) ; celle-ci est régulièrement mise à jour et fournit des éclaircissements et des informations complémentaires sur le contrôle de certaines Exigences.

Si les candidats ne trouvent pas la réponse à leur interrogation dans la FAQ, ils peuvent contacter l'équipe accompagnement Industriels de l'ANS, via l'Espace Authentifié. En retour, l'équipe accompagnement Industriels s'engage à traiter la sollicitation puis à reprendre contact avec les candidats dans les cas suivants :

- Le candidat rencontre une difficulté dans son processus de référencement ;
- Le candidat rencontre un problème lié au traitement de sa candidature ;
- Le candidat rencontre une difficulté avec les vérificateurs de son dossier de référencement, nécessitant une médiation de la part de l'ANS.

4.7. Confidentialité

L'ANS s'engage à conserver comme strictement confidentielles et à ne pas divulguer, révéler ou exploiter, directement ou indirectement, les informations qu'elle peut recueillir sur tout ou partie de la Solution logicielle du candidat. Elle s'engage à reporter cette obligation de confidentialité auprès de tout prestataire de son choix éventuellement appelé à intervenir dans le processus d'attribution du référencement. L'ANS s'engage à ne pas communiquer sur la qualité intrinsèque de la Solution logicielle. Les présentes dispositions s'appliquent en particulier aux résultats obtenus par la Solution logicielle tout au long du processus de référencement décrit plus haut. Elles s'appliquent également à toutes les informations techniques, méthodes, savoir-faire, procédés et documents de quelque nature qu'ils soient, communiqués par l'Editeur à l'ANS. Il est expressément convenu que l'ANS ne saurait être tenue pour responsable de la divulgation d'une information si celle-ci relève du domaine public ou si elle a été obtenue licitement à partir d'autres sources.

Par exception, l'ANS se réserve le droit de communiquer par tout moyen sur l'identité de l'Editeur ou du groupement d'Editeurs ainsi que sur la Solution logicielle pour laquelle une demande de référencement est en cours d'instruction par ses services.

Les règles de confidentialité s'appliquant à compter de l'octroi du référencement sont précisées dans la convention de référencement.

4.8. Protection des données à caractère personnel

Conformément à la réglementation européenne et française sur la protection des données personnelles, l'Editeur est informé que des données à caractère personnel sont susceptibles d'être traitées par l'ANS. Le traitement mis en œuvre a pour finalité l'instruction et le suivi du processus de référencement et de financement, le pilotage du programme de financement et du déploiement auprès des établissements et professionnels de santé des Solutions logicielles référencées par l'ANS, la gestion des sollicitations adressées par l'ANS à l'Editeur dans le cadre du pilotage du programme de référencement et de financement (par ex. des sondages ou questionnaires), le contrôle du bon usage des fonds publics versés à l'Editeur ainsi que la réalisation d'indicateurs statistiques. Des données à caractère personnel sont susceptibles d'être communiquées, dans le cadre des finalités précitées, aux partenaires de l'ANS en charge avec elle du pilotage du dispositif Ségur de financement à l'équipement (CNDA, CNAM, ministère de la santé, ASP, CNSA, CNOP, etc.). La communication de données personnelles, si elle est sollicitée par l'ANS, est nécessaire à l'instruction de la demande de référencement ou à la réalisation des autres finalités précitées. Les données collectées sont conservées pendant la durée du référencement dont bénéficie l'Editeur ainsi que pour les durées d'archivage exigées par la réglementation applicable. L'Editeur dispose d'un droit d'accès, de rectification de ses données ainsi que, dans certains cas, d'effacement, de portabilité,

de limitation, et d'opposition. Les coordonnées du Délégué à la protection des données personnelles de l'ANS sont les suivantes : GIP Agence du Numérique en Santé (Délégué à la protection des données) - 2-10 Rue d'Oradour-sur-Glane 75015 Paris ou par messagerie électronique, à l'adresse suivante : dpo@esante.gouv.fr. L'Editeur dispose également du droit d'introduire éventuellement une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Il est par ailleurs rappelé à l'Editeur, ce que ce dernier reconnait et accepte, qu'il lui appartient de respecter, pour les traitements de données personnelles qu'il met en œuvre, les dispositions du Règlement (UE) 2016-679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et celles de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. En particulier, il appartient à l'Editeur d'assurer l'information de ses clients (établissements et professionnels de santé) sur la communication éventuelle à l'ANS ou ses partenaires, de certaines de leurs données personnelles dans le cadre de la gestion du programme de financement.

4.9. Convention de preuve

De manière générale, l'Editeur et l'ANS reconnaissent aux documents transmis par voie dématérialisée, selon les modalités techniques de transmission déterminées par l'ANS, la qualité de documents originaux et admettent leur force probante, sauf preuve contraire dument rapportée, au même titre qu'un écrit sur support papier. En cas d'utilisation par l'ANS d'un dispositif de signature électronique, l'Editeur et l'ANS conviennent que tout document signé de manière dématérialisée vaut preuve du contenu dudit document et de l'identité des signataires, sauf preuve contraire dument rapportée. Tout document transmis et/ou signé de manière dématérialisée dans les conditions précitées constitue une preuve littérale au sens de l'article 1366 et s. du code civil.

5. GLOSSAIRE

ANS	Agence du numérique en santé, opérateur en charge de la mise en œuvre du présent dispositif
ASP	Agence de services et de paiement, organisme en charge du traitement des demandes de financement et des paiement émises par les Fournisseurs
CDAR2	Clinical Document Architecture, Release 2.0, standard de dématérialisation des documents médicaux électroniques exploitant la syntaxe XML (N1 : données non structurées, N3 : données structurées)
CNAM	Caisse nationale de l'Assurance Maladie
CNDA	Centre national de dépôt et d'agrément
CNSA	Caisse nationale de solidarité pour l'autonomie
CNIL	Commission nationale de l'informatique et des libertés
CNOP	Ordre national des pharmaciens
CPS	Carte de professionnel de santé permettant à son titulaire d'attester de son identité et de ses qualifications professionnelles
CPx	Carte d'identité professionnelle électronique contenant les données d'identification de son porteur (identité, profession, spécialité) et notamment ses situations d'exercice (libéral et salarié), regroupe les carte CPE (personnel d'établissement), CDE (directeur d'établissement) et CPS (professionnels de santé)
DMP	Dossier médical partagé
ES	Etablissement de santé
FINESS	Fichier National des Établissements Sanitaires et Sociaux (FINESS), répertoire de référence pour les établissements à caractère sanitaire, social ou médico-social et de la formation aux professions sanitaires et sociales
HAD	Hospitalisation à domicile
IHE PAM	Integrating the Healthcare Enterprise - Patient Administration Management, nom du flux dédié à la gestion des données administrative des patients
INS	Identité nationale de santé
IRM	Imagerie par résonance magnétique
LDAP	Lightweight Directory Access Protocol (LDAP), protocole permettant de communiquer avec différents types d'annuaires
LPS	Logiciel de Professionnel de Santé
MCO	Médecine, Chirurgie, Obstétrique
MES	Mon Espace Santé
MSSanté	Messagerie sécurisée de santé
MSS-C	Messagerie sécurisée de santé citoyenne (MSS-C) permettant des échanges entre l'usager et les professionnels, Mon espace santé devient opérateur de l'espace de confiance de la MSSanté (le professionnel étant à l'initiative du premier échange)

MSS-Pro	Messagerie sécurisée de santé professionnelle (MSSanté pro) destinée aux professionnels de santé et qui leur permet d'échanger des données ou des documents de santé
NIE	Numéro d'Identification Editeur (NIE) : Numéro d'Identification de l'Editeur, délivré par le Centre National de Dépôt et d'Agrément (CNDA)
NIL	Numéro d'Identification Logiciel (NIL) : Numéro d'Identification Logiciel, délivré par le Centre National de Dépôt et d'Agrément (CNDA) pour l'agrément au titre du composant proposé par l'Editeur
COFRAC	Comité français d'accréditation
PSC	Pro Santé Connect est un fédérateur de fournisseurs d'identité au standard OpenID. Pro Santé Connect permet aux professionnels de s'authentifier soit avec une e-CPS (application mobile) soit avec une carte CPS physique à tous les services numériques de santé raccordés à Pro Santé Connect
PSY	Psychiatrie
RGS	Référentiel général de sécurité
SSR	Soin de suite et de réadaptation