MINISTÈRE
DE LA SANTÉ, DES FAMILLES,
DE L'AUTONOMIE
ET DES PERSONNES HANDICAPÉES
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Ségur du numérique en santé
Systèmes ouverts et non sélectifs (SONS)

Logiciel de gestion d'officine (LGO)
VAGUE 2
Dossier de spécifications de référencement (DSR)

DSR-PHA-LGO-Va2

Annexe II à l'arrêté relatif à un programme de financement destiné à encourager l'équipement numérique des officines
Fonction « Logiciel de gestion d'officine » 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 PHA-LGO-Va2 3
1.2 Définitions 3
2. PÉRIMÈTRE LOGICIEL ÉLIGIBLE AU RÉFÉRENCEMENT 5
3. EXIGENCES LOGICIELLES 6
3.1 Formalisme de description et règles d'application des Exigences 6
3.2 Présentation des Exigences logicielles PHA-LGO-Va2 6
3.2.1 Gestion de l'Identité Nationale de Santé 6
3.2.2 Gestion et partage des documents de santé 11
3.2.3 Consultation et alimentation du DMP / Mon espace santé 14
3.2.4 Gestion de la MSSanté 27
3.2.5 Identification électronique & Pro Santé Connect 31
3.2.6 Conformité aux téléservices 40
3.2.7 Sécurité des SI 42
3.2.8 Autres fonctionnalités 43
3.2.9 Dossier Pharmaceutique (DP) 43
3.2.10 Remontée automatique des documents médicaux par MSSanté 44
3.2.11 Exigences issues de la vague 1 LGO 45
4. MODALITES DE REFERENCEMENT DE LA SOLUTION LOGICIELLE 47
4.1. Principes de référencement de la Solution logicielle 47
4.2. Calendrier du SONS PHA-LGO-Va2 50
4.3. Phase 1 - Dépôt et validation du dossier administratif 50
4.4. Phase 2 - Dépôt de dossier complet de preuves de conformité & instruction par l'ANS 52
4.5. Phase 3 - Signature de la convention Ségur par l'Editeur et attribution du référencement 54
4.6. Espace Authentifié, Support et FAQ 54
4.7. Confidentialité 55
4.8. Protection des données à caractère personnel 56
4.9. Convention de preuve 56
5. GLOSSAIRE 57

1. PRÉSENTATION ET DÉFINITIONS

1.1 Présentation du dispositif SONS PHA-LGO-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 « LGO » (Logiciels de gestion d'officine) 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-PHA-LGO-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-PHA-LGO-Va2 (présent document)**, qui présente les modalités de présentation et d'instruction des demandes de référencement ;
- **Le document d'appel à financement AF-PHA-LGO-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'officine bénéficiaire 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-PHA-LGO-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.

MES / DMP : Mon espace santé / Dossier Médical Partagé

Périmètre vague 1 ou vague 2 : le Périmètre vague 1 et le Périmètre vague 2 renvoient à l'onglet « Exigences » du REM-PHA-LGO-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 la Prestation Ségur vague 2 dont le périmètre décrit à la Section 3 de l'AF -PHA-LGO-Va2.

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 présent DSR s'adresse aux fournisseurs de Logiciels de Gestion d'Officine (LGO), équipant les professionnels exerçant en pharmacie d'officine de ville. Ces fournisseurs peuvent s'associer à d'autres logiciels en sous-traitance ou en cotraitance afin de répondre à l'ensemble des exigences contenues dans le référentiel d'exigences et de scénarios de conformité REM-PHA-LGO-Va2.

Sont considérés comme LGO, les logiciels qui contiennent les fonctions minimales suivantes :

- Facturation Assurance Maladie (système SESAM-Vitale accessible par carte vitale et carte CPS) validé par le GIE SESAM-Vitale ;
- Compatibilité avec le dossier pharmaceutique validé par le Conseil National de l'Ordre des Pharmaciens (CNOP) ;
- Historique des délivrances de médicaments (ordonnancier) ;
- Base de données des médicaments et produits de santé ;
- Gestion des stocks de médicaments ;

Les autres logiciels utilisés par les pharmaciens de ville ne sont pas éligibles au référencement Ségur, notamment :

- Logiciels ou solutions connexes au LGO et liés à une spécificité de l'activité pharmaceutique ;
- Logiciels de comptabilité ;
- Logiciels exclusivement dédiés à la gestion administrative de la pharmacie ;
- Systèmes experts d'aide à la dispensation ;
- Systèmes de sauvegarde et archivage des données ;
- Logiciels ou solutions d'un dispositif médical ;
- Logiciels ou téléservices fournis par une institution publique (nationale ou régionale).

	Secteur d'activités Logiciel	Secteur d'activités Logiciel
Périmètre couvert	**Officine de ville**	• **LGO seul** • **LGO avec d'autres logiciels** en sous-traitance / co-traitance
Périmètre non couvert	Pharmacie à usage intérieur (PUI)	• Logiciel non LGO seul

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-PHA-LGO-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 6 du code de la santé publique.

Cas des solutions déjà référencées en vague 1

Dans le REM-PHA-LGO-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.*

3.2 Présentation des Exigences logicielles PHA-LGO-Va2

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

- Gestion de l'Identité Nationale de Santé
- Gestion et partage des documents de santé
- Consultation et alimentation du DMP / Mon espace santé
- Gestion de la MSSanté
- Identification électronique & Pro Santé Connect
- Conformité aux téléservices
- Sécurité des SI
- Autres fonctionnalités
- Dossier Pharmaceutique (DP)
- Remontée automatique des documents médicaux par MSSanté
- Exigences issues de la vague 1 LGO

3.2.1 Gestion de l'Identité Nationale de Santé

3.2.1.1 Objectifs pour le LGO en vague 2

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.

Pour rappel, l'utilisation de l'Identité Nationale de Santé (INS) pour référencer les données de santé est une obligation réglementaire depuis le 1er janvier 2021.

Dans le cadre du déploiement de la vague 1 du Ségur numérique, le dispositif « Sentinelle » a permis de définir de nouvelles Exigences destinées à faciliter la gestion de l'INS par les professionnels de santé au sein de leurs logiciels, sur la base des retours terrain. En vague 2, les objectifs sont les suivants :

- Systématiser la qualification de l'Identité Nationale de Santé (INS) dans les Logiciels pour éviter les erreurs d'identitovigilance.
- Simplifier au maximum la procédure pour les professionnels (réduire les clics, automatiser ce qui peut l'être).
- Faciliter la compréhension des retours du téléservice INSi pour fluidifier leur traitement.

3.2.1.2 Fonctionnalités couvertes par les exigences vague 2

N°	GESTION DE L'IDENTITE NATIONALE DE SANTE- Fonctionnalités du périmètre Vague 2	Exigences associées
1.1	**Gestion code officiel géographique (COG) 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
1.2	**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
1.3	**Production d'indicateurs**	
	Gestion des traces pour sécuriser l'usage	SC.INS.17
1.4	**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 Faciliter la recherche d'une identité dans la base patient Création d'une nouvelle identité dans le LGO	SC.INS.05 SC.INS.13 SC.INS.14 SC.INS.15 SC.INS.19 SC.INS.22 SENTINELLE.02 SENTINELLE.05 SENTINELLE.07

Le corpus documentaire INS, et notamment le Guide d'implémentation, a été revu à la lumière des enseignements du terrain : 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, notamment pour :

- 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.

3.2.1.3 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) /Mon espace santé 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.

3.2.1.4 Présentation détaillée des principales évolutions

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 discordance entre l'INS et les traits présents sur le dispositif à haut niveau de confiance. Cela peut s'expliquer du fait qu'une commune ait 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.

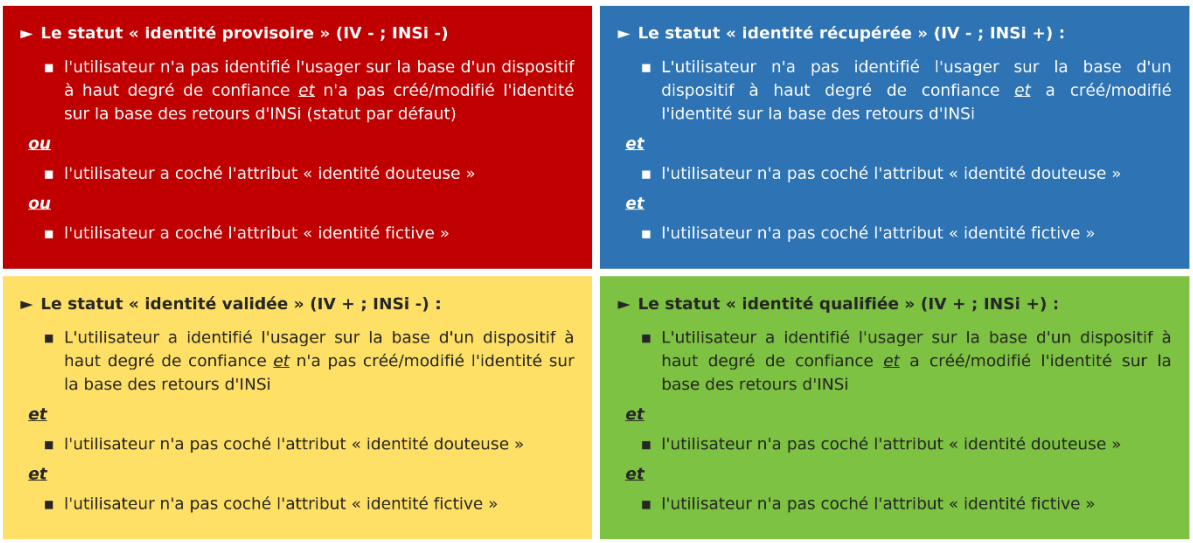
Il est essentiel de distinguer la récupération de l'INS via la carte Vitale, qui permet d'obtenir une identité au statut « récupéré » (et non "qualifiée"), de l'utilisation de l'appli carte Vitale. Cette dernière permet de récupérer et de qualifier de manière plus rapide et efficace. Une fois l'identité 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 d'emblée 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.

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.

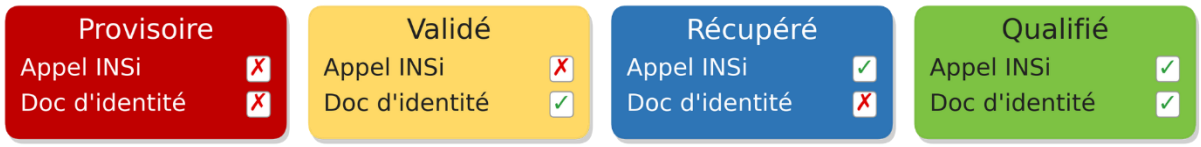
Les statuts de l'identité sont :

- 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.

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.

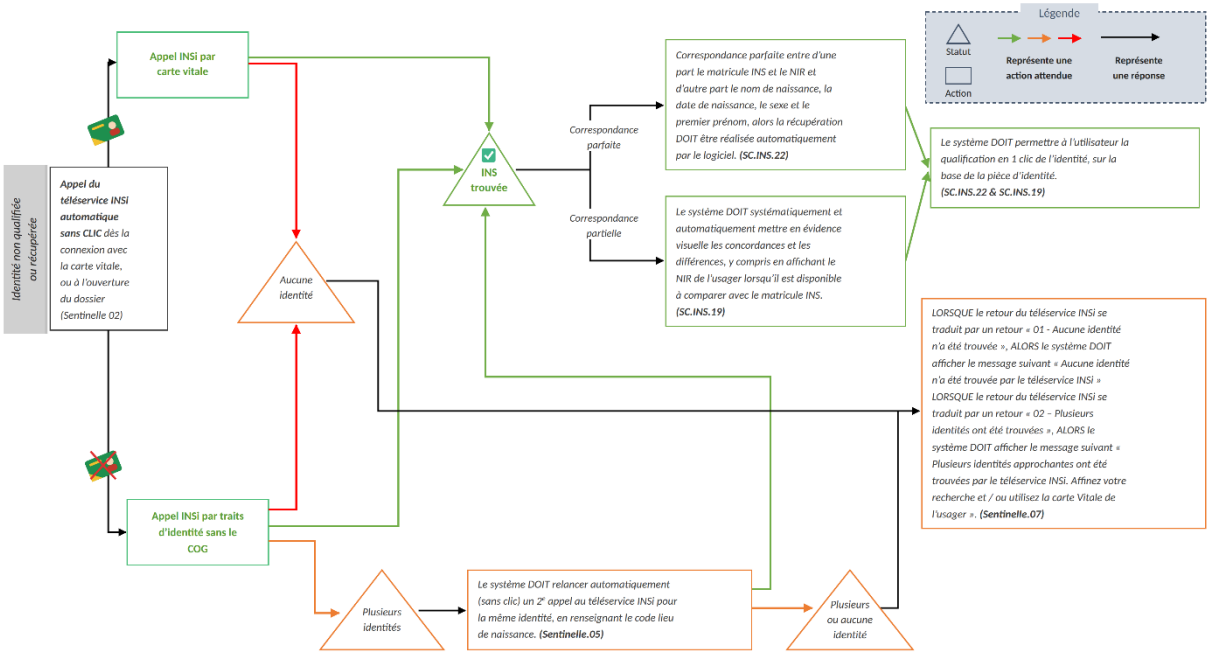
En cas de retour unique du téléservice INSi, les concordances et divergences entre les données sont mises en évidence visuellement, permettant à l'utilisateur de valider l'identité en un clic.

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 ou qualifiée depuis 4 ans,
- Le matricule INS est de type NIA, à l'occasion d'un nouvel événement système.

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

Suggestions d'implémentation de la qualification de l'INS dans les LGO

Les prochaines préconisations sont des suggestions, non obligatoires à implémenter pour l'éditeur. Elles permettront de faciliter l'utilisation du logiciel pour le professionnel de santé.

Préconisation 1 :
Pour permettre aux professionnels de caractériser les identités nécessitant un traitement particulier, le système peut permette l'emploi des attributs homonyme, douteux et fictif.

- *L'attribut « Identité homonyme » a pour objet de faciliter l'identification et la gestion des identités à fort taux de ressemblance (homonymes avérés ou identités approchantes) qui doivent faire l'objet d'une vigilance particulière de la part des acteurs de santé. Il peut être associé à chacun des 4 statuts précédemment définis et n'est pas, sauf exception (exemple : modification a posteriori d'un des traits stricts), modifié au cours des éventuels changements de statut d'une identité. Cet attribut peut être diffusé à l'ensemble des applications du domaine d'identification.*
- *L'attribut « Identité douteuse » permet de tracer l'existence d'un doute sur la véracité de l'identité recueillie (usager confus, suspicion d'utilisation frauduleuse d'identité, situation sanitaire exceptionnelle, etc.). Il ne peut être associé qu'à un statut Identité provisoire. Dans le cas où il est associé à une identité ayant précédemment reçu un statut de confiance supérieur, il entraîne la rétrogradation du statut en Identité provisoire. Et, si le matricule INS et son OID étaient liés, ils seront supprimés ou rendus invalides.*
- *L'attribut « Identité fictive » peut uniquement être associé au statut Identité provisoire. Il a pour objet de faciliter la gestion :*
  - *Des identités dites sensibles, faisant l'objet d'une règlementation particulière en termes d'anonymisation des prises en charge ;*
  - *D'autres situations de création d'identités fictives (traits imaginaires attribués à un patient incapable de décliner son identité, tests informatiques, formation, etc.).*

Seuls les attributs douteux et homonymes peuvent être utilisés simultanément, les attributs fictifs et douteux ne peuvent être cumulés.

Préconisation 2 :
Le système peut ne pas nécessairement forcer la qualification de l'INS dès l'ouverture du dossier patient. L'ouverture rapide de la fenêtre de qualification INS pourrait perturber la saisie des éléments dans le dossier patient. L'appel au téléservice doit se lancer automatiquement dès ouverture du dossier patient, mais une fois les informations récupérées, la qualification peut s'effectuer à un moment plus opportun (par exemple, à la fin de la consultation, lors de l'envoi des documents via Mon espace santé et /ou MSS) ;

Préconisation 3 :
Le système peut afficher un message d'explication à destination du professionnel de santé lorsque celui-ci valide un document et que l'INS n'est pas qualifiée, voir renvoyer au processus de qualification.

3.2.2 Gestion et partage des documents de santé

Le présent paragraphe concerne la gestion et le partage des documents de santé en vague 2, avec 2 sujets principaux :

1) Considérations générales sur la gestion des documents dans le LGO
2) Production des notes de vaccination

3.2.2.1 Considérations générales sur la gestion des documents dans le LGO

3.2.2.1.1 Objectifs pour le LGO 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/Mon espace santé 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 /Mon espace santé ou reçus par MSSanté :
    - Informer l'utilisateur qu'un document du DMP/Mon espace santé 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 ;
    - Identifier parmi tous les documents du logiciel les documents importés depuis le DMP/Mon espace santé et la MSSanté, afin que l'utilisateur soit conscient de sa provenance ;
- 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/Mon espace santé ou reçus par MSSanté :
    - Identifier parmi tous les documents du logiciel les documents envoyés vers le DMP/Mon espace santé 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) ;
    - Limiter les re-saisies et préremplir les documents produits avec les données présentes dans le dossier patient ;
- Etendre le périmètre des « documents Ségur ».

3.2.2.1.2 Fonctionnalités couvertes par les exigences vague 2 :

N°	GESTION ET PARTAGE DES DOCUMENTS DE SANTE - Fonctionnalités du périmètre Vague 2	Exigences associées
2.1	**Affichage des documents au format CDA R2 N1 et N3**	
	• Mise en visibilité de la copie PDF encapsulée qui doit être affichée de préférence lors de l'ouverture pour les documents CDA R2 N3. Possibilité de basculer vers le format CDA R2 N3 sur action de l'utilisateur • Affichage des métadonnées des documents CDA R2 N3 et PDF associés sur une seule ligne dans l'espace documentaire	**SC.CDA/VISU.03** **SC.CDA/VISU.01** **SC.CDA/DD.15**
2.2	**Production des documents au format CDA R2 conformes au CI-SIS**	
	• Production des documents au format CDA R2 N1 conformément au volet du CI-SIS • Pré-remplissage des documents avec les données présentes dans le dossier patient • Production des documents au format CDA intégrant le Datamatrix et marquage « INS à scanner » • Production d'un document de test rapide d'orientation diagnostique, conformément au volet du CI-SIS	**LGC.MDV.03** **SC.DOC.03** **SC.CDA/VISU.04** **TROD.01**
2.3	**Navigation dans le dossier patient local et identification des documents importés depuis / exporté vers le DMP /Mon espace santé et la MSSanté**	
	Tri des documents importés et produits, a minima, selon le type et la date de l'acte. Les informations utilisées pour le tri doivent être à défaut celles issues du CDA • Identification dans le dossier patient des documents importés depuis le DMP /Mon espace santé et la MSSanté • Identification dans le dossier patient des documents déjà exportés vers le DMP /Mon espace santé • Absence de blocage de l'interface graphique de l'utilisateur pendant les requêtes aux services numériques en santé (DMP, Annuaire santé, Pro Sante Connect, INSi et Ordonnance Numérique, MSSanté, ApCV) • Affichage (sans clic) du statut de l'identité du patient (provisoire, validée, récupérée (si possible), qualifiée), au niveau de l'interface "dossier patient"	**SC.CDA/INT.04** **SC.CDA/INT.17** **SC.CDA/INT.08** **SC.DMP/HISTO.01** **LGC.DMP/UX.10** **SC.DMP/UX.11**
2.4	**Information de l'existence et visualisation d'une version plus récente d'un document déjà intégré dans le dossier patient**	
	• Information de l'utilisateur lors de la consultation du DMP d'un patient si une version plus récente d'un document intégré au dossier patient est disponible dans le DMP /Mon espace santé • Accès direct à la dernière version du document et possibilité d'intégration dans le LGO et possibilité de visualiser les versions précédentes.	**SC.CDA/DD.06** **SC.CDA/VISU.02**
2.5	**Eviction des conflits entre documents identiques**	
	• Afin d'éviter les doublons, le système vérifier la cohérence de tout document CDA reçu (via le DMP / Mon espace santé ou MSS) et présent dans le système. • S'assurer de la cohérence des CDA R2 N1, pdf/A-1, CDA R2 N3 d'un même document et qu'ils sont produits à partir de la même source de données. • Génération du pdf rattaché au courriel MSSanté à partir des mêmes données que celles utilisées dans le document CDA de l'IHE_XDM	**SC.CDA/INT.18** **SC.CDA/DD.02** **SC.CDA/DD.12**

3.2.2.1.3 Présentation détaillée des principales évolutions

Affichage des documents au format CDA R2 N1 et N3

En vague 1, les documents structurés étaient produits au format CDA R2 niveau 3, sans intégrer le PDF du compte rendu. Cette approche nécessitait la production de deux documents distincts (un CDA R2 N1 contenant le PDF et un CDA R2 N3 structuré), ce qui pouvait entraîner des doublons, une consommation accrue d'espace de stockage et des difficultés de lisibilité dans les espaces documentaires des logiciels des professionnels de santé ou de Mon espace santé.

En vague 2, les documents structurés, notamment pour les comptes rendus d'examens de biologie médicale, intègrent directement le PDF du compte rendu au sein du document CDA R2 niveau 3. Le LGO devra être en mesure de consommer ces documents et d'en assurer un affichage adapté. L'affichage du PDF encapsulé devra être privilégié afin de restituer le document tel qu'il a été produit. En complément, le LGO pourra proposer un affichage des données structurées à l'aide de sa propre feuille de style, tout en permettant à l'utilisateur de revenir, si nécessaire, à la présentation d'origine du document.

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

La gestion des documents de santé doit in fine permettre le partage et l'échange 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 et échange s'effectue à deux niveaux :

- A travers l'alimentation du DMP / Mon espace santé
- Par envoi via messagerie sécurisée au médecin traitant, au prescripteur s'il y a lieu, à tout professionnel dont l'intervention dans la prise en charge du patient paraît pertinente à l'émetteur 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 du ministre chargé de la santé et de l'accès aux soins, en tenant compte du déploiement des mises à jour logicielles permettant de systématiser ces partages et échanges numériques, avec la possibilité laissée au professionnel de retenir un envoi sur demande légitime du patient.

Pré-remplissage des documents produits par le LGO à partir des informations du dossier patient

Afin de faciliter la production des documents cités dans la « Liste de documents Ségur » du REM-PHA-LGO-Va2, le système doit préremplir les champs dudit document avec des informations déjà présentes dans le dossier patient. Le professionnel de santé doit pouvoir les modifier/supprimer si nécessaire après leur intégration.

Rappel : préconisations pour le nommage de documents

Cette partie permet de recenser les règles de nommage pour les objets de messages sécurisés via MSSanté et documents envoyés vers DMP/MES. Les objectifs de la normalisation de l'objet du courriel sont de

- *Permettre au logiciel du professionnel de santé (LPS) récepteur d'identifier le type du document envoyé ainsi que le patient concerné*
- *Au professionnel de santé destinataire du courriel d'identifier le type de document et le patient concerné dans le cas où le courriel ne serait pas automatiquement traité par son LPS (sans devoir nécessairement ouvrir la pièce jointe).*

Il est préconisé que le logiciel suive la recommandation de l'exigence ECO.2.1.3 du ***Référentiel socle MSSanté #2 - Clients de Messageries Sécurisées de Santé*** *concernant le format de l'objet du courriel MSS :*

E	**ECO.2.1.3**  L'objet du courriel DOIT respecter le format suivant : XDM/1.0/DDM+<libellé> <NOM> <prenom> <date de naissance> Tous les champs sont obligatoires à l'exception du champ <date de naissance> qui est optionnel.

Il est aussi préconisé que le logiciel suive les recommandations du ***Ci-sis_service_volet-echange-documents-sante_v1.8.*** *de la section 3.2.4. Ces recommandations présentent la structuration des messages, la taille totale maximale de caractères et la structuration préconisée de la chaîne de caractère de l'objet du message. La section 3.2.8 est aussi recommandée afin de structurer le message de réponse.*

<u>Nommage des documents envoyés via MSSanté</u>
Il est préconisé que le logiciel suive l'exigence ECO 2.1.1 du ***Référentiel socle MSSanté #2 - Clients de Messageries Sécurisées de Santé.*** *Cette exigence présente les règles de transmission d'un document de santé.*

De plus, l'exigence ECO.2.1.5 de ce même référentiel présente les règles de création d'un PDF/A-1 rattaché au courriel MSSanté.

Par rapport au volet échange de documents de santé [CI-ECH-DOC], aucune normalisation complémentaire n'est imposée sur le nom des documents xml au format CDA.

Nommage des documents envoyés dans Mon espace santé

Il est recommandé que le logiciel suive l'exigence EX_2.1-1020, EX_2.1-1030 et EX_2.1-1040 du guide d'intégration Service DMP intégré au LPS ***SEL-MP-037.*** *Ces exigences indiquent que les spécificités nécessaires du champ « titre » d'un document, définies dans la norme XDS.b.*

3.2.2.2 La production des notes de vaccination

3.2.2.2.1 Objectifs pour le LGO en vague 2

Les notes de vaccination dans les LGO ont été introduites dans la vague 1 avec leur production au format CDA R2 N3, conformément au volet vaccination du CI-SIS. Ces notes de vaccination, produites par le professionnel, ont pour vocation d'être concaténées au sein de Mon espace santé en un historique de vaccination, permettant le suivi de la vaccination des patients. La vague 2 ajoute :

- L'accès facilité au schéma vaccinal présent sur le site du ministère chargé de la santé ;
- Le pré remplissage de la note de vaccination à partir des informations scannées sur les boîtes de vaccin.

3.2.2.2.2 Fonctionnalités couvertes par les exigences vague 2

	Production de la note de vaccination – fonctionnalités du périmètre Vague 2	Exigences associées
2.9	**Schéma vaccinal**	
	Lien vers le schéma vaccinal	SC.VACC/SCHEMA.01
2.10	**Production de la note de vaccination**	
	Production d'une note de vaccination conformément à la version du CI-SIS en vigueur Pré remplissage de la note de vaccination à partir des informations scannées sur la boîte de vaccin	SC.CDA/DD.23 SC.VACC/NOTE.05

3.2.2.2.3 Présentation détaillée des principales évolutions

La note de vaccination (CDA R2 N3) permet de coder le vaccin administré à un patient. Cette note de vaccination est créée par le professionnel de santé à l'aide de son logiciel puis transmise au DMP /Mon espace santé qui consolide toutes les notes de vaccination du patient dans son historique des vaccinations.

Afin de faciliter la production de ce document, le logiciel doit savoir produire la note de vaccination conformément au volet « Note de vaccination », en facilitant sa production via le pré-remplissage de ce document par la lecture du Datamatrix de la boite de vaccin.

Pour faciliter cette étape pour le professionnel de santé, l'éditeur fournira une documentation listant au moins un dispositif de lecture du Datamatrix du commerce compatible avec son système.

Un lien vers le schéma vaccinal depuis le logiciel doit être implémenté.

3.2.3 Consultation et alimentation du DMP / Mon espace santé

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

1. Les enjeux d'enregistrement de **l'information et du consentement du patient** ;
2. **La consultation, directement depuis le logiciel métier, du DMP /Mon espace santé du patient** qui constitue un des objectifs majeurs de la vague 2 du Ségur numérique ;
3. **L'alimentation systématique du DMP /Mon espace santé du patient** avec les documents qui lui sont remis à chaque épisode de prise en charge, en renforçant les fonctionnalités déjà présentes en vague 1 ;
4. 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.

3.2.3.1 Information et consentement du patient

3.2.3.1.1 Objectifs pour le LGO 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 par défaut à l'utilisateur habilité authentifié, le temps de l'acte (délivrance, entretien, ...) et peut être étendu pour des besoins de suivi au long cours à l'ensemble des professionnels habilités de l'officine, ainsi que dans la durée jusqu'à révocation demandée par le patient.

Préconisation :
Dans le cadre d'une prise en charge patient, plusieurs demandes d'autorisation ou consentement peuvent être requises : non opposition à l'alimentation du DMP / Mon espace santé, consentement à la consultation du DMP / Mon espace santé, voire d'autres consentements.

Afin d'en faciliter la gestion pour les professionnels, il est possible de ***regrouper*** *ces autorisations dans une interface dédiée (par exemple, dans la gestion administrative patient), y compris en mutualisant les cases à cocher, et avec la possibilité d'effectuer les renvois pertinents vers cette interface depuis les différentes interfaces métiers lorsque cela est pertinent pour faciliter l'usage.*

3.2.3.1.2 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
3.1	**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/Mon espace santé et respect des droits d'accès qui en résulte	SC.DMP/CONF.06 SC.DMP/CONF.06.BIS SC.DMP/CONF.09.BIS OFF.DMP/CONF.06

3.2.3.1.3 Présentation détaillée des principales évolutions

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

Pour l'alimentation du DMP / Mon espace santé :

- Valeur par défaut : le professionnel / l'officine 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 / Mon espace santé :

- Valeur par défaut : le professionnel / l'officine ne peut pas consulter le DMP / MES
- Patient informé et consentant : il peut consulter le DMP / MES, dans les limites du périmètre et de la durée définis au moment du recueil (cf. ci-dessous)
- Patient informé et non consentant : il ne peut pas consulter le DMP / MES

Le consentement à la consultation est recueilli pour l'ensemble du personnel habilité de l'officine (voir exigence SC.DMP/CONF.06). L'utilisateur définit la durée du consentement :

- **Valeur par défaut : « Pour l'acte en cours »** : le système enregistre localement le consentement pour tous les utilisateurs de la pharmacie pendant 72 heures, puis le consentement expire.
- **Valeur étendue : « Pour le suivi au long cours »** : le système exige la saisie d'un motif (champ texte libre, non vide), puis enregistre localement le consentement pour tous les utilisateurs de la pharmacie jusqu'à sa révocation par le patient.

Quelle que soit la durée du consentement, l'autorisation d'accès positionnée au niveau du DMP suit la même règle (exigence OFF.DMP/CONF.06) :

- Le système positionne une autorisation individuelle d'accès (TD0.3) pour chaque utilisateur qui consulte effectivement le DMP pendant la validité du consentement ;
- Il supprime cette autorisation lors de la première authentification de l'utilisateur après l'expiration d'un délai de 72 heures suivant son positionnement ;
- Dans le cadre du suivi au long cours, il positionne à nouveau l'autorisation lors de la consultation suivante, de façon totalement transparente pour le professionnel de santé : le consentement ayant été recueilli dans le LGO, aucune action ni aucun nouveau recueil ne lui est demandé.

Exemples d'implémentation UI/UX de recueil du consentement compatibles avec l'exigence du REM pour le consentement à la consultation du DMP/MES dans le logiciel métier :

Illustration 1 : Gestion centralisée du consentement, quelle que soit le la temporalité (Pour l'acte en cours ou Pour le suivi au long cours)

1. Accès depuis le dossier administratif du patient, espace consentements :



2. Enregistrement du consentement sur le dossier du patient :

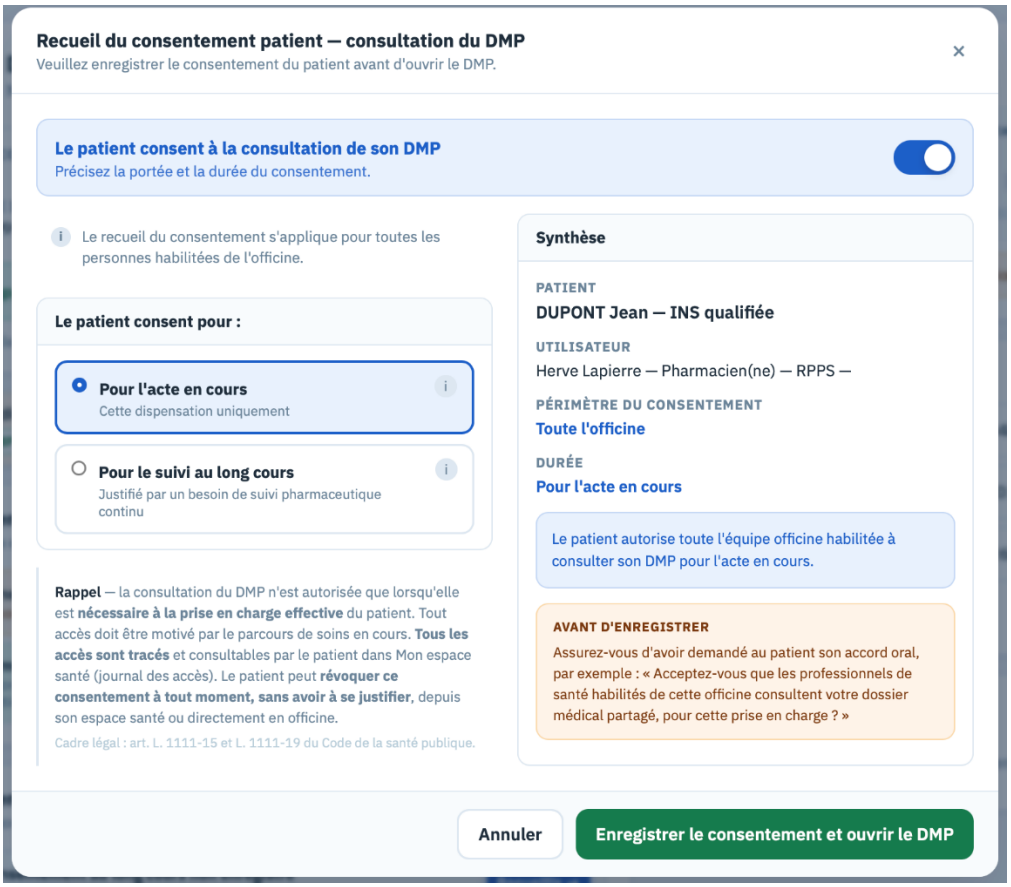


Illustration 2 : Recueil avec UX simplifié dans le cadre du recueil pour l'acte en cours

1. Accès depuis le dossier patient, espace DMP :



2. Recueil du consentement directement pour l'acte en cours :



Illustration 3 : Traçabilité du motif pour un consentement pour le suivi au long cours : champ conditionnel



3.2.3.2 Consultation du DMP / Mon espace santé

3.2.3.2.1 Objectifs pour le LGO 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.

Le principal objectif de la de la vague 2 est de 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), et ainsi :

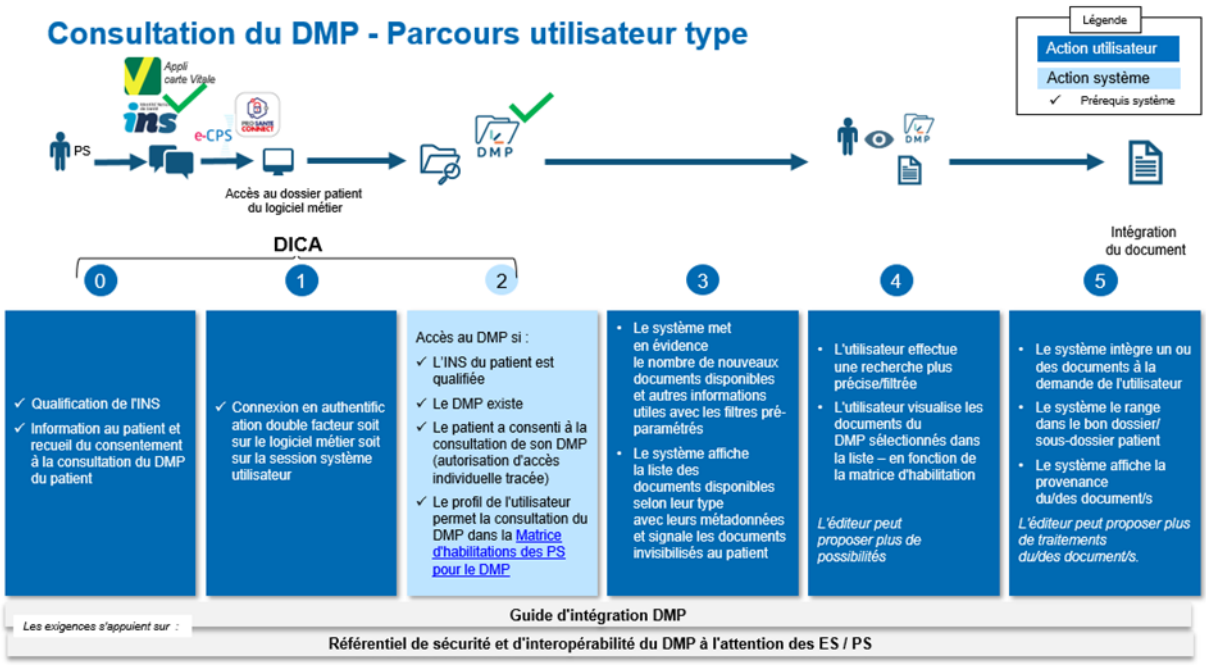
- Le professionnel **doit savoir sans clic s'il peut consulter le DMP / Mon espace santé de son patient.** Dans le cas où il ne peut consulter, il doit pouvoir, sur action de sa part, connaitre la ou les cause(s) de son incapacité à consulter **(cf. Conditions cumulatives explicitées ci-dessous)**.
- Le professionnel **doit connaître la provenance et le statut des documents** envoyés et intégrés (provenance, nouvelle version disponible, etc.).
- Le professionnel **doit disposer facilement du nombre de documents nouvellement alimentés par des professionnels, patients et structures tierces 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 /Mon espace santé afin de pouvoir les visualiser, en mettant en avant les documents invisibles au patient, qu'il a vocation à rendre visibles suite à l'annonce.
- Le professionnel **peut manuellement intégrer un document de Mon espace santé pour le visualiser** et l'intégrer dans son logiciel.

3.2.3.2.2 Fonctionnalités couvertes par les exigences vague 2

	CONSULTATION DE MON ESPACE SANTE - Fonctionnalités périmètre Vague 2	Exigences associées
3.2	**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 /Mon espace santé et extraction de ces informations • Le système DOIT être homologué CNDA correspondant au "Guide d'intégration DMP"	SC.DMP/CONF.21 SC.DMP/CONF.14 SC.DMP/CONF.15
3.3	**Autorisation de consultation du DMP /Mon espace santé et information rapide de l'utilisateur sur son contenu**	
	• Vérification des conditions cumulatives d'accès au DMP / Mon espace santé • Visualisation sans clic de la capacité à consulter le DMP / Mon espace santé • Affichage synthétique des métadonnées des documents présents dans le DMP du patient • Mise en évidence des documents invisibles au patient dans la liste • Masquage et démasquage des documents aux autres professionnels dans le DMP du patient • Recherche multicritère dans la liste des documents du DMP / Mon espace santé	SC.DMP/CONF.16 SC.DMP/UX.13 SC.DMP/UX.14 SC.DMP/UX.14.BIS SC.DMP/UX.14.TER SC.DMP/UX.27
3.4	**Intégration de documents du DMP /Mon espace santé dans le dossier patient local**	
	- Sélection multiple de documents du DMP /Mon espace santé de la liste présentée et intégration dans le dossier patient	SC.DMP/UX.31

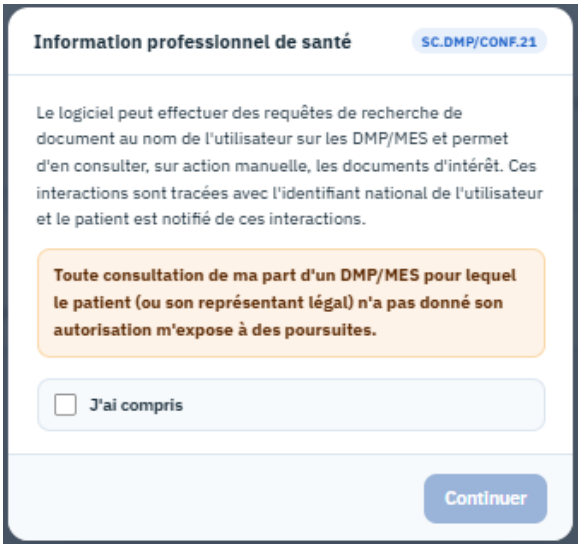
3.2.3.2.3 Présentation détaillée des principales évolutions

Parcours utilisateur pour la consultation du DMP



Le système doit responsabiliser le professionnel de santé en affichant un message indiquant que toute consultation de sa part d'un DMP/MES pour lequel un patient (ou son représentant légal) n'a pas donné son autorisation l'expose à des poursuites. Ce message sera affiché lors de la première connexion au logiciel (post mise à jour Ségur) et rappelé à période paramétrable pour l'informer de la transmission de ses identifiants au DMP /Mon espace santé (valeur par défaut = 180 jours).

Ci-dessous, illustrations d'interface d'information professionnel de santé (SC.DMP/CONF.21) :





La case « J'ai compris » doit être décochée par défaut.

Le système pourra prolonger automatiquement cet accès sans réinterroger le professionnel de santé tous les 180 jours.

Actions logicielles pour la consultation du DMP /Mon espace santé

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.

1. **Tracer le consentement du patient à la consultation du DMP/Mon espace santé (cf. paragraphe dédié ci-dessus)**

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 les professionnels de santé accèdent 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 / Mon espace santé, le logiciel ne lance aucune transaction de consultation et peut afficher cette information à l'utilisateur connecté (cf. illustrations ci-dessous).

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 :



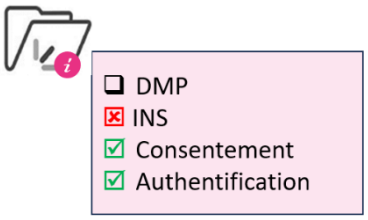
Exemples d'icônes traduisant le fait que l'utilisateur **a la capacité de consulter** le DMP / MES du patient

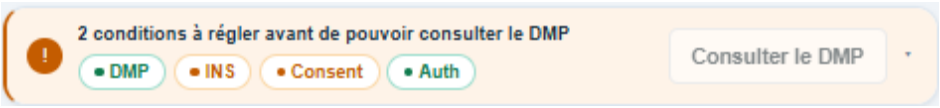
Exemples d'icônes traduisant le fait que l'utilisateur **n'a pas la capacité de consulter** le DMP / MES du patient

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

Ci-dessous des exemples 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, par exemples :

DMP :

- Indisponibilité technique du DMP => Info sur indisponibilité
- 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

Authentification :

- Je ne suis pas authentifié avec un moyen d'identification sécurisé
- => Je m'authentifie en avec Pro Santé Connect[1]

Illustration à titre indicatif :



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/Mon espace santé, il est nécessaire que le logiciel positionne automatiquement l'autorisation individuelle d'accès du professionnel à l'aide de son RPPS. L'autorisation individuelle d'accès permet au DMP/Mon espace santé 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/Mon espace santé et l'afficher au patient. Cette autorisation individuelle est supprimée lors de la première authentification de l'utilisateur après l'expiration d'un délai de 72 heures suivant son positionnement. Dans le cadre du suivi au long cours, elle est positionnée à nouveau lors de la consultation suivante, de façon transparente pour l'utilisateur (voir section 3.2.3.1.3).

Le logiciel doit rester fonctionnel lorsqu'il effectue les requêtes au DMP/Mon espace santé.

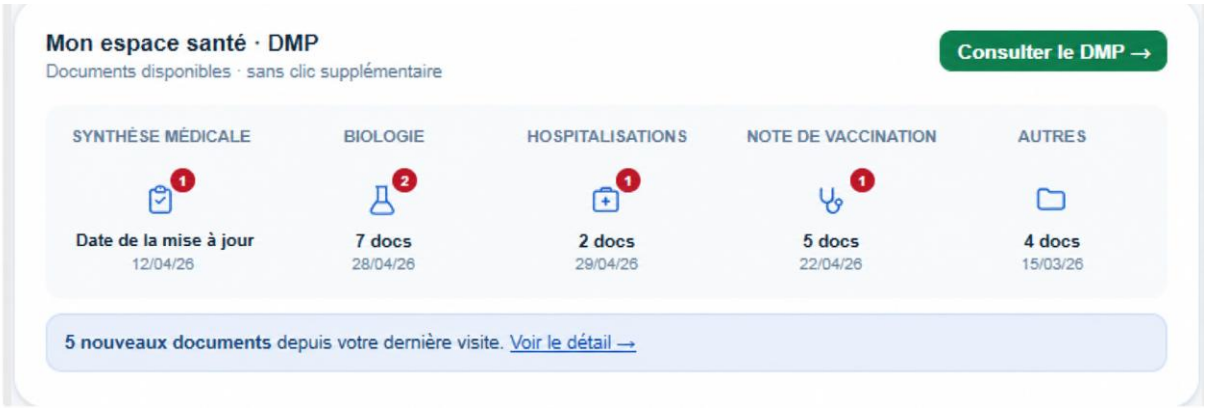
[1] La consultation du DMP peut se faire également avec une authentification CPS. Néanmoins, compte-tenu des usages terrain en officine et de la généralisation de Pro Santé Connect comme moyen d'authentification au sein du LGO, c'est ce moyen d'authentification qui est illustré et recommandé dans ce cas d'usage.

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

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/une interface 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 peut tout de même permettre à l'utilisateur de rechercher des documents dans le DMP/Mon espace santé par critères. A noter : il est possible d'effectuer des recherches/filtres sur tous éléments des métadonnées des documents : titre du document, type de document, nom de l'auteur, profession de l'auteur, date, visibilité, etc.

Exemple d'interface affichant le nombre de documents versés au DMP/Mon espace santé du patient depuis la dernière consultation par le professionnel :



4. Masquage et démasquage des documents aux autres professionnels

Le logiciel doit permettre au professionnel de masquer ou démasquer un ou plusieurs documents sélectionnés du DMP du patient à l'attention des autres professionnels habilités, en mobilisant la transaction TD3.3a du DMP. Cette fonctionnalité, distincte du mécanisme d'invisibilité au patient, permet d'organiser le partage entre professionnels en cohérence avec les règles de confidentialité applicables (par exemple : restreindre temporairement l'accès à un document avant une consultation d'annonce).

5. 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).

6. 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 pour l'intégration du ou des documents dans son logiciel. Le logiciel va enregistrer le document issu du DMP/Mon espace santé dans sa base de données, notamment en fonction de sa date, de son type.

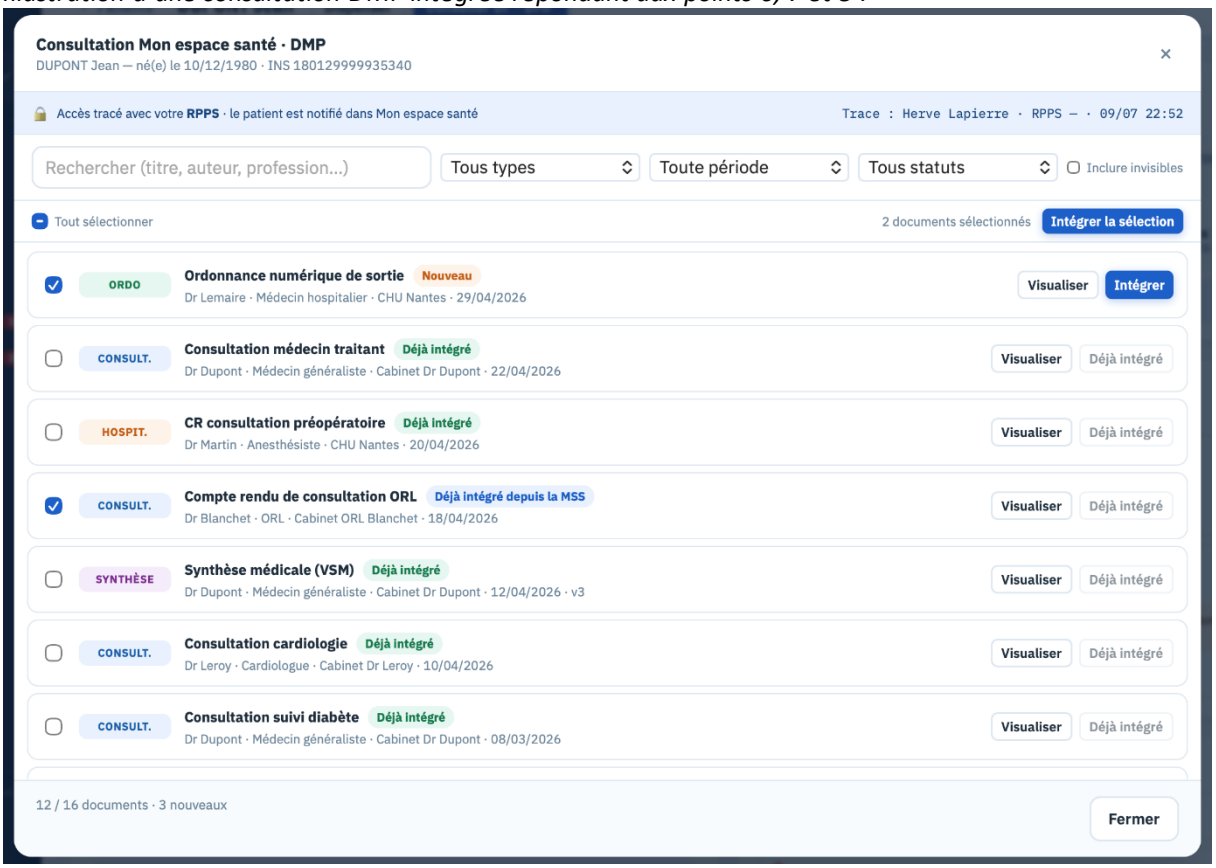
7. Éviter les doublons

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.

8. Indiquer la provenance

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

Illustration d'une consultation DMP intégrée répondant aux points 6, 7 et 8 :



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 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.

3.2.3.3 Alimentation du DMP / Mon espace santé

3.2.3.3.1 Objectifs pour le LGO en vague 2

En vague 1, l'objectif a été de généraliser l'envoi systématique et sécurisé dans le DMP/Mon espace santé 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 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** et manuellement des documents présents dans le logiciel métier datant d'épisodes de santé antérieurs dit « historiques » n'ayant pas été préalablement envoyés au DMP / Mon espace santé, sous condition d'avoir au préalable qualifié l'INS du patient.
- S'assurer que la fonction de suppression des documents dans le DMP/Mon espace santé soit effective, si erreur dans le document menant à modification ou suppression définitive du document dans le logiciel producteur.

3.2.3.3.2 Fonctionnalités couvertes par les exigences vague 2

	ALIMENTATION DE MON ESPACE SANTE - Fonctionnalités périmètre Vague 2	Exigences associées
3.5	**Alimentation systématique de Mon espace santé**	
	• Envoi systématique et automatique sans action utilisateur des documents au DMP/Mon espace santé avec une exécution différée et en tâche de fond. • Possibilité pour l'utilisateur de bloquer ou annuler l'ordre d'envoi au DMP/Mon espace santé avant sa validation et pendant la période de différée d'exécution. • Mise en attente des documents lorsque la connexion au DMP/Mon espace santé n'est pas possible puis exécution des ordres d'envoi lorsque la connexion est rétablie	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
3.6	**Alimentation ponctuelle de Mon espace santé**	
	• Alimentation du DMP de documents issus d'actes réalisés à une date antérieure à la date du jour et stockés dans le dossier patient du système	SC.DMP/HISTO.03 SC.DMP/HISTO.05
3.7	**Suppression d'un document du DMP en cas d'erreur d'alimentation ou de demande du patient**	
	• Possibilité de supprimer un document du DMP/Mon espace santé en cas d'erreur d'alimentation ou de demande du patient concerné	SC.DMP/CONF.03

3.2.3.3.3 Présentation détaillée des principales évolutions

Alimentation différée au DMP/Mon espace santé

Afin de limiter les actions en arrière-plan et ainsi optimiser les performances du logiciel, l'alimentation au DMP/Mon espace santé doit être exécutée en différé par rapport à la validation du document par le professionnel de santé (SC.DMP/ALI/PROG.02). Cette action pourra donc être lancée le soir ou entre deux patients : il est suggéré de laisser à l'utilisateur la possibilité de paramétrer cet ordre d'envoi.

L'objectif de cette fonctionnalité est de fluidifier l'envoi des documents au DMP/Mon espace santé du point de vue utilisateur, lui permettre de modifier/corriger un document avant que celui-ci ne soit alimenté dans le DMP/Mon espace santé, ainsi que de permettre le rattrapage de l'envoi si indisponibilité technique du DMP.

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

3.2.3.4.1 Objectifs pour le LGO 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 leurs 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. Aucun document ne doit rester durablement dans le DMP/Mon espace santé, sans que le patient n'y ait accès. Il est donc impératif d'encourager la remise en visibilité par le professionnel de santé annonceur.

Ainsi, le logiciel doit alors :

- Permettre au **professionnel qui accompagne le patient ayant bénéficié d'une 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.

3.2.3.4.2 Fonctionnalités couvertes par les exigences vague 2

	INVISIBILISATION DE MON ESPACE SANTE - Fonctionnalités périmètre Vague 2	Exigences associées
3.8	**Autorisation de consultation du DMP/Mon espace santé et information rapide de l'utilisateur sur la présence de documents invisibles et permettre la remise en visibilité**	
	Affichage des documents qui sont invisibles au patient et possibilité de les rendre visible Fonction de recherche et/ou de filtrage basée sur des critères issus des métadonnées XDS du DMP/Mon espace santé (documents invisibles, période donnée…).	SC.DMP/UX.14.BIS SC.DMP/UX.27

3.2.3.4.3 Présentation détaillée des principales évolutions

Rappel des fondamentaux concernant la mise en visibilité et remise en visibilité des documents alimentés au DMP/Mon espace santé

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/Mon espace santé 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 ;
- 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/Mon espace santé 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 en adaptant les délais à la réalité des usages :

- Un **mode d'envoi (préexistant) 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 aux **professionnels qui participent au parcours de soins** de **remettre en visibilité le document** « manuellement » directement dans leurs logiciels habituels ;
- Une « **remise en visibilité automatique » par le DMP/Mon espace santé 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/Mon espace santé 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, ou le cas échéant qu'il n'y ait pas de perte de chance dans le parcours patient par absence d'information.

(Au moment de la publication du SONS PHA-LGO-Va2, le dispositif de remise en visibilité automatique n'est pas encore opérationnel ; toutefois, ses modalités d'application sont en cours de finalisation pour un déploiement dans les mois suivants).

3.2.4 Gestion de la MSSanté

3.2.4.1 Objectifs pour le LGO en Vague 2

La messagerie sécurisée de santé (MSSanté) est la modalité privilégiée et réglementaire 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 la configuration de la messagerie pour l'utilisateur ;
- Faciliter l'identification de la bonne adresse MSSanté d'un correspondant, y compris quand ce dernier dispose de plusieurs adresses en permettant une recherche sur tous les attributs possibles de cette adresse, et en affichant des retours complets de la recherche permettant de sécuriser que l'interlocuteur retourné est bien celui attendu ;
- Simplifier l'intégration des documents de santé reçus par MSSanté et la réception de mises à jour de documents par MSSanté ;
- Identifier, parmi les documents reçus par MSSanté, ceux qui ont déjà été intégrés dans le logiciel ;
- Assurer l'interopérabilité des logiciels avec l'ensemble des opérateurs de messagerie ;
- Assurer la traçabilité des opérations MSSanté.

3.2.4.2 Fonctionnalités couvertes par les exigences vague 2

	Gestion de la MSSanté - Fonctionnalités du périmètre Vague 2	Exigences associées
4.1	**Intégration de l'annuaire santé**	
	Recherche multicritère de l'adresse MSSanté d'un correspondant en interrogeant l'annuaire MSSanté depuis le LGO et affichage de l'ensemble des champs de l'annuaire de façon à maximiser les chances de l'utilisateur de trouver le bon interlocuteur Permettre d'enregistrer, pour un patient donné, les professionnels qui sont amenés à le prendre en charge.	SC.MSS/CONF.20 SC.MSS/UX.41 LABEL.06 ANN/va1.01 ANN/va1.02 ANN/va1.04
4.2	**Intégration et gestion des documents reçus par MSSanté**	
	Faciliter l'intégration des documents reçus, notamment via MSS, en exploitant les métadonnées de l'archive IHE XDM	MSS/UX.42
4.3	**Autoconfiguration de la boîte aux lettres MSS**	
	Configuration automatique des paramètres de connexion au serveur de messagerie	SC.MSS/CONF.04
4.4	**Envoi sécurisé vers la messagerie de Mon espace santé d'un patient**	
	Permettre la fermeture du canal de communication avec le patient après l'envoi du message Sélection d'un usager destinataire du message via une liste construite à partir de la base des usagers connus du système ou depuis le dossier patient Génération automatique de l'adresse MSSanté Citoyenne du patient lors de la rédaction d'un message	SC.MSS/CONF.21 SC.MSS/UX.32
4.5	**Production et conservation de traces MSS**	
	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). Traçage des actions utilisateurs réalisées avec la MSSanté et son contenu	SC.MSS/CONF.17 SC.MSS/CONF.18 MSS/va1.14
4.6	**Interopérabilité avec les opérateurs de MSSanté**	
	• Utilisation de protocoles sécurisés pour l'échange de données par MSSanté • Standardisation de la cinématique de connexion à une BAL MSSanté • Autoconfiguration de la BAL • Interface d'envoi de messages utilisant le protocole SMTP conforme à la RFC 5321 • 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 • Traitement des erreurs techniques lors du processus de connexion et d'authentification • 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 • Positionnement des-têtes SMTP (invisibles de l'utilisateur) exploités par l'ANS à des fins statistiques : présence d'un INS qualifié, type de document CDA échangé, référence produit • 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	SC.MSS/CONF.01 SC.MSS/CONF.03 SC.MSS/CONF.04 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.14 SC.MSS/CONF.15 SC.MSS/CONF.16 SC.MSS/CONF.22 SC.MSS/CONF.27 SC.MSS/CONF.28
4.7	**Information patient prévention**	
	Envoi automatique d'un message MSSanté vers l'adresse MS citoyenne du patient lors de la dispensation d'un antibiotique, contenant un lien vers le site Antibio'malin (sante.fr).	LGO/OFF.01

3.2.4.3 Présentation détaillée et suggestions d'implémentation

Intégration des documents reçus depuis MSS

Schéma illustrant les processus attendus dans l'exigence MSS/UX.42 selon les différents statuts possibles de l'identité :

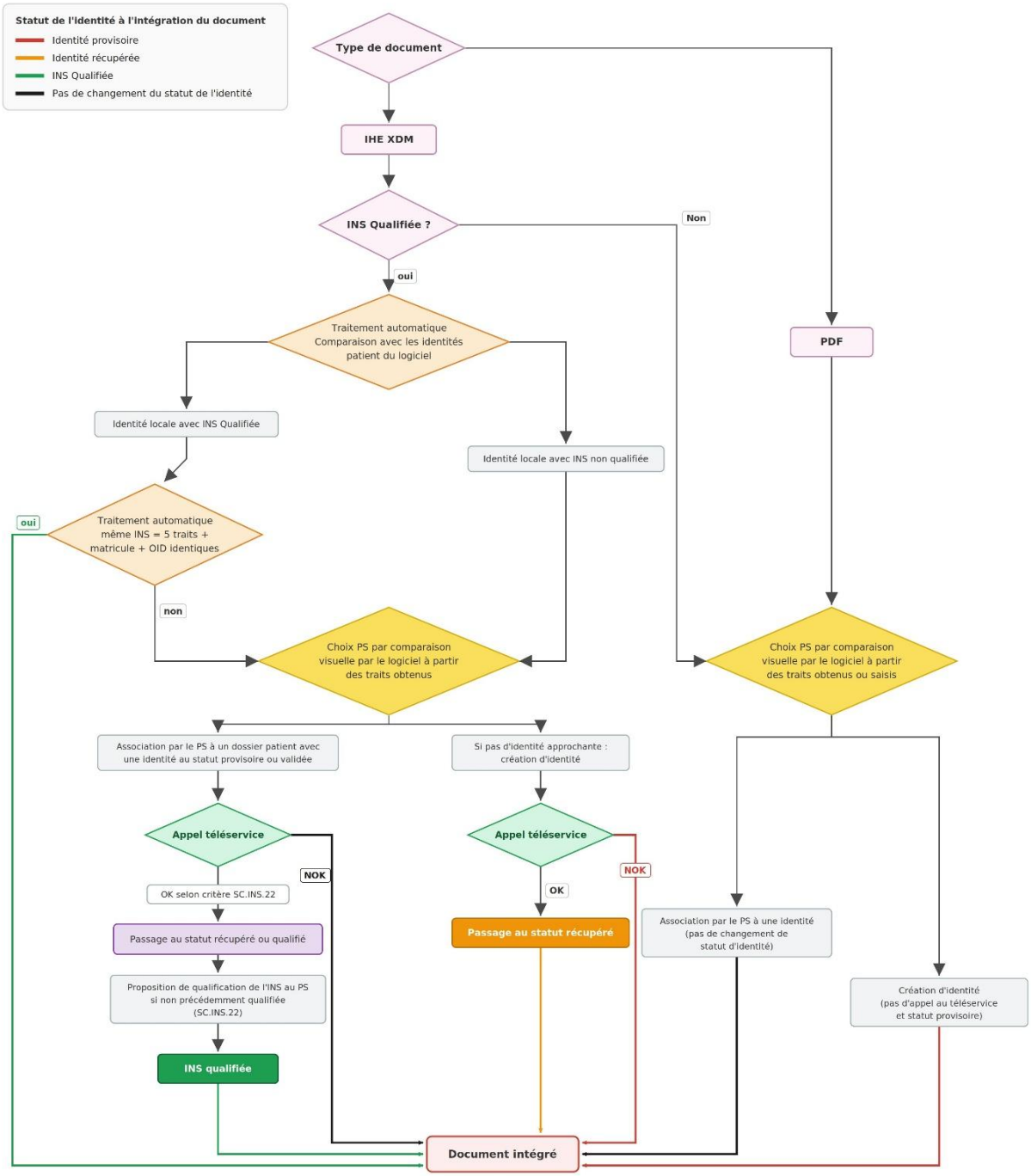
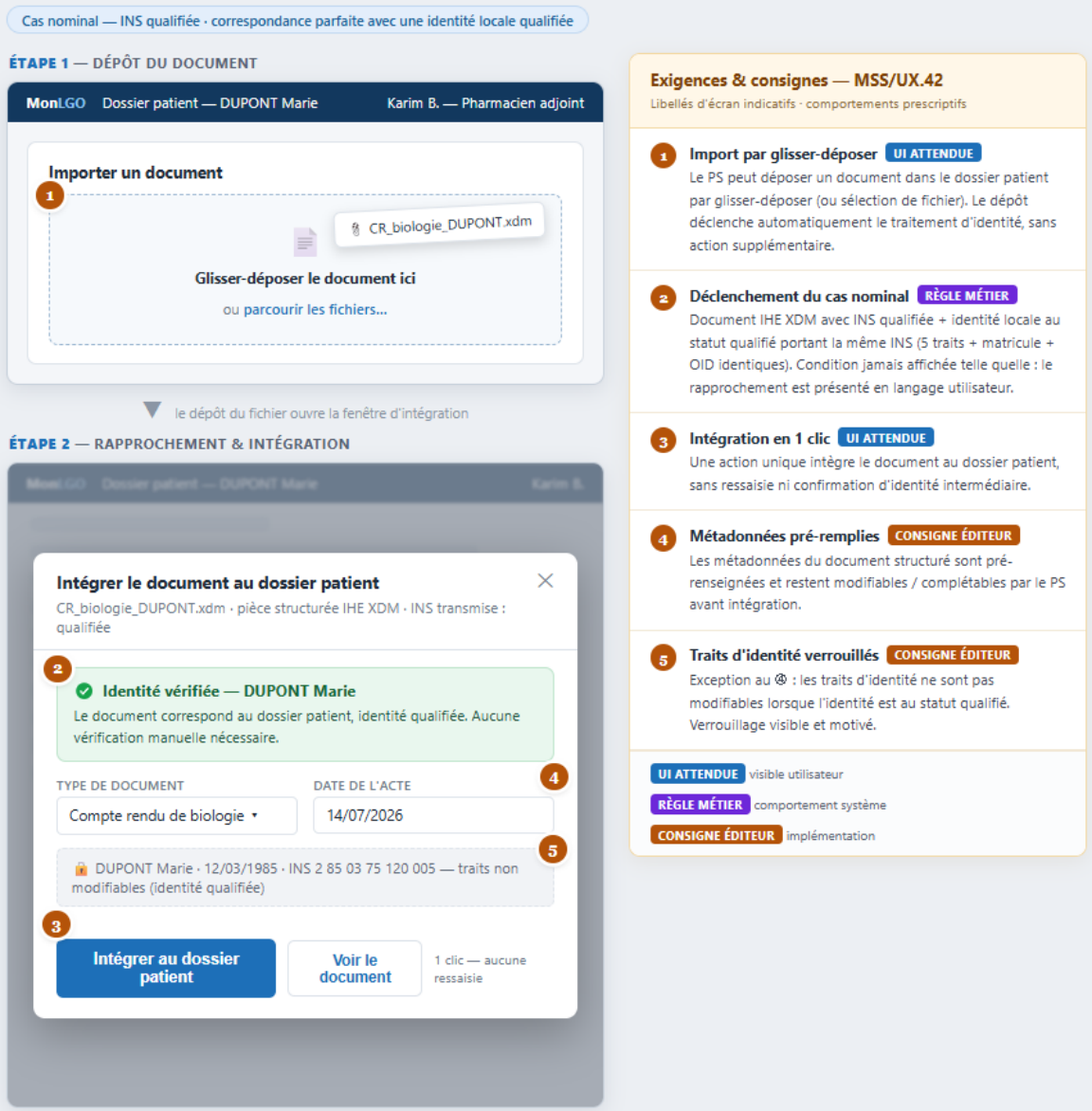


Schéma illustrant le processus d'intégration des documents dans le dossier patient attendu dans l'exigence MSS/UX.42.



Suggestions d'implémentation MSS pour la sécurité des SI

Les prochaines préconisations sont des suggestions, non obligatoires à implémenter pour l'éditeur. Elles permettront de faciliter l'utilisation du logiciel pour le professionnel de santé.

Préconisation 1 :
Lors d'une connexion IMAP, le système peut utiliser le capability SASL-IR pour transmettre l'Access Token en une seule transaction comme défini dans le RFC 4959.

Préconisation 2 :
Si le système propose une IHM présentant des messages reçus, cette dernière peut proposer d'utiliser un mode d'affichage sous forme de conversation.

Suggestions d'implémentation MSS pour faciliter les usages

Préconisation :
Pour distinguer facilement, dans la liste des messages reçus, les messages émis par des professionnels des messages émis par des patients, il est proposé d'utiliser des logos simples d'emblée compréhensibles des

professionnels tels que pour les messages provenant de professionnels et des messages provenant de patients.

3.2.5 Identification électronique & Pro Santé Connect

3.2.5.1 Objectifs pour les LGO 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 service Pro Santé Connect (PSC) pour l'identification électronique des acteurs de la santé. Pro Santé Connect est un fournisseur d'identité au standard OpenID Connect, qui s'appuie sur plusieurs moyens d'identification électronique. Pro Santé Connect permet ainsi aux professionnels de santé de s'identifier à tous les services numériques de santé qui lui sont raccordés grâce à plusieurs moyens d'authentification électronique, tels que la e-CPS (application mobile), la carte CPS physique, ou via des « clés de sécurité » (périphériques externes type carte de technologie FIDO2, appairables au compte Pro Santé Connect).

L'objectif est donc de pouvoir sécuriser et simplifier l'identification électronique des professionnels en intégrant Pro Santé Connect et en limitant les étapes d'authentification aux services numériques en santé. Par conséquent, il est souhaité de généraliser l'authentification par PSC pour l'accès au LGO ainsi qu'aux services numériques en santé, notamment les services socles : MSSanté, DMP, …

- Pour le LGO, il s'agit ainsi de proposer une identification simple, sécurisée et unifiée, permettant aux utilisateurs habilités de se connecter au LGO puis aux services socles sans réauthentifications inutiles, tout en garantissant la traçabilité des accès et la conformité au référentiel Pro Santé Connect ainsi qu'au référentiel d'identification électronique des personnes physiques (RIE PP).
    - Dans ce cadre, l'authentification via Pro Santé Connect permet d'assurer une continuité d'accès entre le LGO et les services numériques en santé, sans rupture dans le parcours utilisateur.
- La vague 2 couvre non seulement l'intégration de PSC comme fournisseur d'identité, mais également les attendus liés à l'Espace de confiance PSC, à la gestion des sessions en environnement nomade, à l'enrôlement du moyen d'identification électronique utilisé avec PSC, ainsi qu'au fonctionnement en mode dégradé lorsque le service PSC n'est pas disponible.
- Les services déléguant leurs authentifications à Pro Santé Connect bénéficient de la 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.

Dans ce cadre, la généralisation de Pro Santé Connect ne se limite pas à un changement de mécanisme d'authentification : elle implique une évolution des modalités d'usage au sein des logiciels de gestion d'officine, en particulier dans des environnements caractérisés par un fonctionnement multi-postes et des usages fortement nomades.

La mise en œuvre d'une authentification forte systématique pour l'accès aux services numériques de santé doit ainsi être conciliée avec les contraintes opérationnelles de l'officine, où les professionnels sont amenés à se déplacer fréquemment d'un poste à un autre au cours de leur activité.

3.2.5.2 Enjeux d'usage en officine et principe de la session nomade

La mise en œuvre de Pro Santé Connect en officine doit donc répondre à un double objectif structurant : garantir un haut niveau de sécurité des accès tout en préservant la fluidité des usages dans un environnement multi-postes.

En effet, l'organisation du travail en officine repose sur :

- des postes de travail multiples ;

- des professionnels amenés à se déplacer fréquemment au cours d'une même activité ;
- des contraintes de continuité de service fortes.

La généralisation d'une authentification forte via Pro Santé Connect constitue ainsi un levier majeur de sécurisation des accès aux données de santé depuis les LGO, mais introduit également une exigence nouvelle : éviter toute rupture excessive dans les usages métier liée à la multiplication des authentifications.

La Vague 2 du Ségur introduit ainsi un modèle cible reposant sur les principes suivants :

- Une authentification forte initiale (2FA) via Pro Santé Connect, s'appuyant sur un moyen d'identification électronique (MIE), typiquement une *clé de sécurité* (technologie FIDO2) appairée au compte Pro Santé Connect du professionnel ;
- Une gestion de session sécurisée, permettant de maintenir l'état authentifié de l'utilisateur sur une durée limitée ;
- Un usage en itinérance (session nomade), permettant à un même professionnel de retrouver un accès fluide à son environnement de travail sur plusieurs postes ;
- Des mécanismes de sécurité associés, notamment en matière de durée de session, d'inactivité et de réauthentification.

Ce modèle vise à répondre aux objectifs suivants :

- Garantir une authentification forte et homogène pour l'accès aux services socles ;
- Renforcer la sécurisation des accès aux données de santé depuis les LGO ;
- Permettre des usages fluides en contexte officinal multi-postes, en limitant les réauthentifications inutiles.

Il repose sur un principe structurant : authentification forte au démarrage, usages fluides au quotidien.

Pré-requis structurant : L'accès aux services numériques en santé via Pro Santé Connect repose sur l'inscription au RPPS (Répertoire Partagé des Professionnels de Santé) du professionnel. Cette inscription est la condition d'accès et conditionne l'ensemble du parcours décrit ci-après, en particulier pour les préparateurs en pharmacie pour lesquels la démarche d'inscription est en cours.

3.2.5.3 Fonctionnalités couvertes par les exigences vague 2

	Identification électronique & Pro Santé Connect - Fonctionnalités du périmètre Vague 2	Exigences associées
5.1	**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) ;
	• Usage de Pro Santé Connect pour la connexion aux services socles sans réidentification ;
		SC.PSC.01
		SC.PSC.02
		SC.PSC.08

5.2	**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
5.3	**Session nomade et reprise de session sur poste partagé**	
	• Reprise de session entre postes via badge NFC d'un MIE PSC compatible (type FIDO2) • Verrouillage automatique d'un poste après une période d'inactivité applicative paramétrable • Invalidation de la session applicative après une période d'inactivité prolongée sur l'ensemble des postes • Changement de session par un autre utilisateur sur un poste, par présentation de son MIE FIDO2 PSC compatible en NFC, avec verrouillage de la session précédente • Affichage d'un menu d'enrôlement du MIE FIDO2 PSC compatible lors de la première authentification d'un utilisateur non encore associé à un MIE dans le Système	SC.PSC.23 SC.PSC.21 SC.PSC.27 SC.PSC.25 SC.PSC.24

5.4	**Mode dégradé en cas d'indisponibilité du service Pro Santé Connect**	
	• Mode dégradé activable par un administrateur en cas d'indisponibilité de PSC, autorisant l'authentification locale en 2FA avec MIE FIDO2 pour 24 h maximum	SC.PSC.26

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

Précisions sur la session nomade et la continuité de service en officine

Trois mécanismes spécifiques à l'environnement officinal méritent d'être précisés :

- **Reprise de session entre postes par badge NFC** (SC.PSC.23) : après une authentification initiale en 2FA via Pro Santé Connect avec un MIE FIDO2 PSC compatible, l'utilisateur peut rejoindre un autre poste en présentant simplement son MIE en NFC (1FA). Le système ouvre alors l'accès sur le nouveau poste en 3 secondes maximum, sans nouvelle authentification PSC complète.
- **Changement de session par un autre utilisateur** (SC.PSC.25) : lorsqu'un utilisateur est connecté à une session sur un poste, un second utilisateur peut prendre la main en présentant son propre MIE FIDO2 en NFC ; la session précédente est alors verrouillée. Ce mécanisme est essentiel en officine pour permettre la rotation rapide entre pharmaciens et préparateurs sur un même poste.
- **Mode dégradé en cas d'indisponibilité de PSC** (SC.PSC.26) : lorsqu'un administrateur active ce mode, les utilisateurs peuvent s'authentifier localement au LGO en 2FA avec leur MIE FIDO2, sans passer par PSC, pour une durée maximale de 24 heures. Ce mode permet la continuité de service en cas d'incident PSC, en interdisant les sessions nomades en 1FA (le 2FA reste obligatoire). L'administrateur reçoit une notification automatique et peut désactiver manuellement le mode dès que PSC redevient disponible.

Les durées d'inactivité (verrouillage du poste à partir de 30 min, invalidation globale de la session jusqu'à 4 h) sont détaillées dans le REM. Le mécanisme d'enrôlement à la première authentification PSC est illustré dans la sous-section *"Parcours d'enrôlement de référence et pré-requis associés"* ci-dessous.

3.2.5.4 Parcours d'enrôlement de référence et pré-requis associés

Pré-requis d'enrôlement

L'enrôlement du professionnel et de son moyen d'identification électronique (MIE) repose sur les pré-requis suivants, qui doivent être satisfaits préalablement à l'utilisation du LGO en mode authentifié :

- Inscription au RPPS (Répertoire Partagé des Professionnels de Santé) du professionnel — condition d'accès à l'ensemble des services numériques en santé via Pro Santé Connect. Une intensification de l'inscription des préparateurs en pharmacie est en cours dans le cadre du plan d'accompagnement Ségur.
- Activation matérielle de la clé de sécurité (FIDO2) avec définition d'un code PIN par le professionnel.
- Enregistrement de la clé de sécurité sur le compte Pro Santé Connect du professionnel.
- Association de la clé au compte utilisateur du LGO, pour permettre la reconnaissance de l'utilisateur lors des authentifications ultérieures.

Le parcours illustré ci-dessous, déroulé dans un environnement logiciel reproduisant des conditions réelles d'usage, présente un parcours utilisateur de référence pour l'enrôlement et l'activation de la clé de sécurité. Il démontre la faisabilité d'un parcours intégré au sein du LGO, permettant de guider le professionnel de bout en bout sans rupture significative entre les environnements (logiciel métier, mire Pro Santé Connect, fenêtre système d'activation de la clé). Les éditeurs restent libres d'adopter une autre logique d'agencement dès lors qu'ils accompagnent l'utilisateur dans la satisfaction des pré-requis d'enrôlement et que l'expérience utilisateur reste fluide.

En effet, ce processus mobilise plusieurs environnements et interfaces distincts (logiciel métier, mire Pro Santé Connect, système d'exploitation ou solution d'activation du moyen d'identification électronique), susceptibles de générer des ruptures dans l'expérience utilisateur.

Dans ce contexte, il est attendu que les éditeurs mettent en œuvre un parcours permettant :

- de guider l'utilisateur de bout en bout, étape par étape ;
- d'assurer la continuité du parcours, malgré les changements d'environnement ;
- de limiter les situations de blocage, en particulier lors des premiers usages.

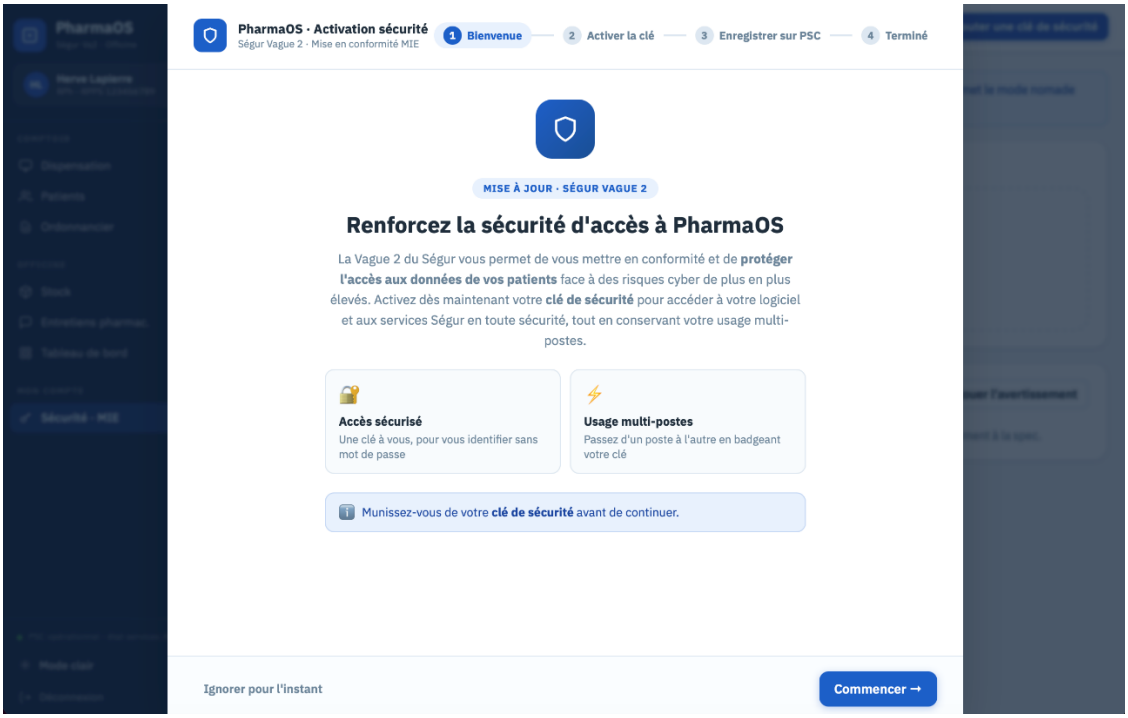
Au-delà de la phase initiale de déploiement, ce parcours a vocation à être mobilisé de manière récurrente, notamment dans les situations suivantes :

- arrivée d'un nouveau professionnel ;
- renouvellement ou remplacement d'une clé de sécurité ;
- perte ou dysfonctionnement d'un moyen d'identification électronique.

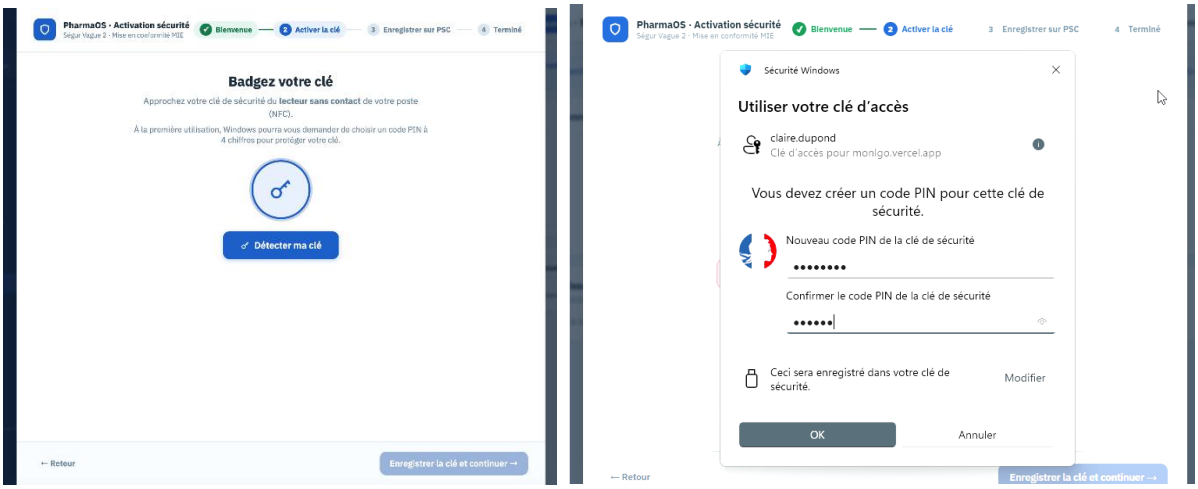
Il est ainsi attendu que les solutions proposées permettent d'autonomiser les utilisateurs, en leur offrant un parcours compréhensible, reproductible et sécurisé dans le temps.

Ce parcours constitue un repère visant à garantir un niveau minimal de qualité en matière d'accompagnement utilisateur, en permettant de guider de manière claire et continue les différentes étapes nécessaires à l'activation et à l'utilisation de la clé de sécurité dans le cadre de Pro Santé Connect. Les éditeurs peuvent l'adapter et l'optimiser en fonction des spécificités de leur solution, des choix techniques retenus et des modalités d'accompagnement mises en place (intégration dans le LGO, parcours assisté, supports complémentaires, etc.).

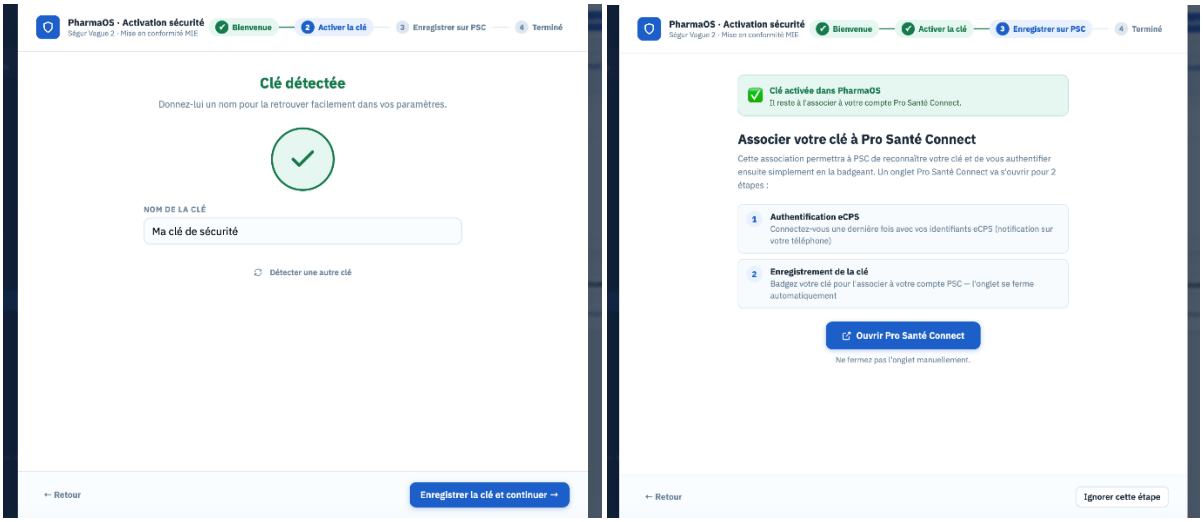
Etape 1 : L'utilisateur ouvre sa session après la mise à jour Ségur : un parcours d'enrôlement se déclenche (report possible dans une limite de temps donné)



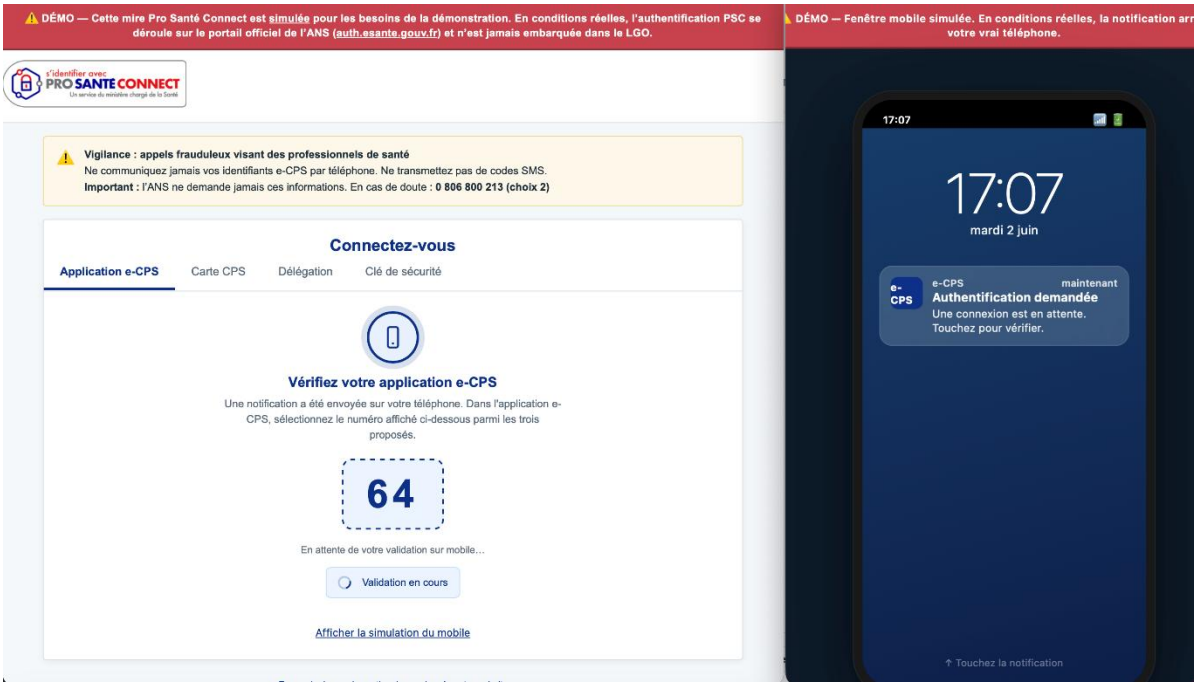
Etape 2 : L'utilisateur badge sa clé de sécurité, et saisie son code PIN (création d'un nouveau code PIN si clé de sécurité jamais activée, comme ci-dessous)



Etape 3 : Une fois la clée détectée et asssociée au compte utilisateur, l'utilisateur clique sur « Ouvrir Pro Santé Connect » pour s'authentifier et ainsi associer son identifié Pro Santé Connect à son compte LGO

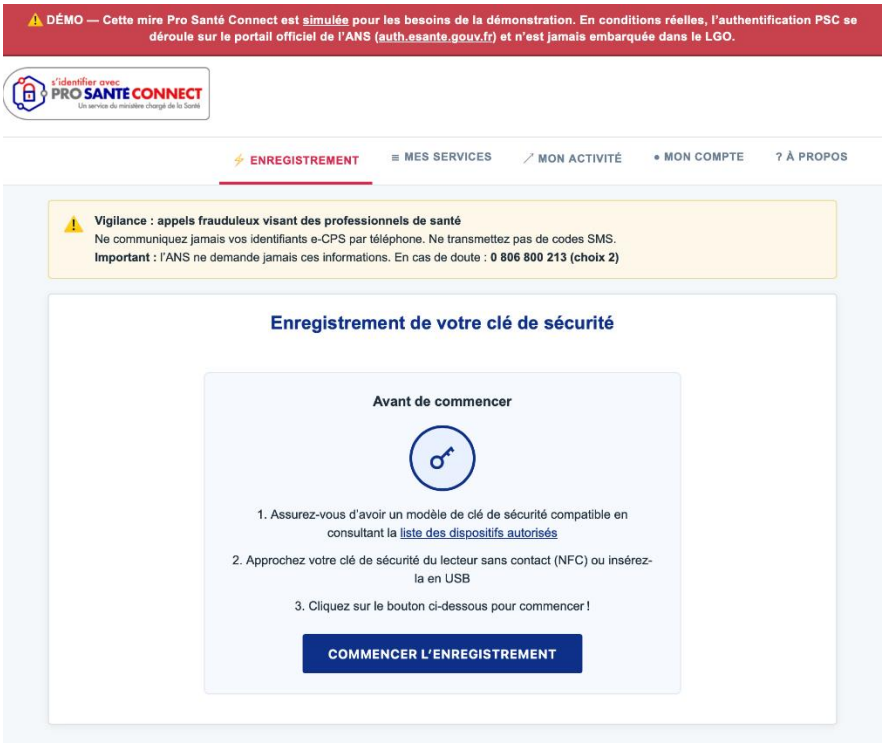


Etape 4 : L'utilisateur s'authentifie avec sa eCPS

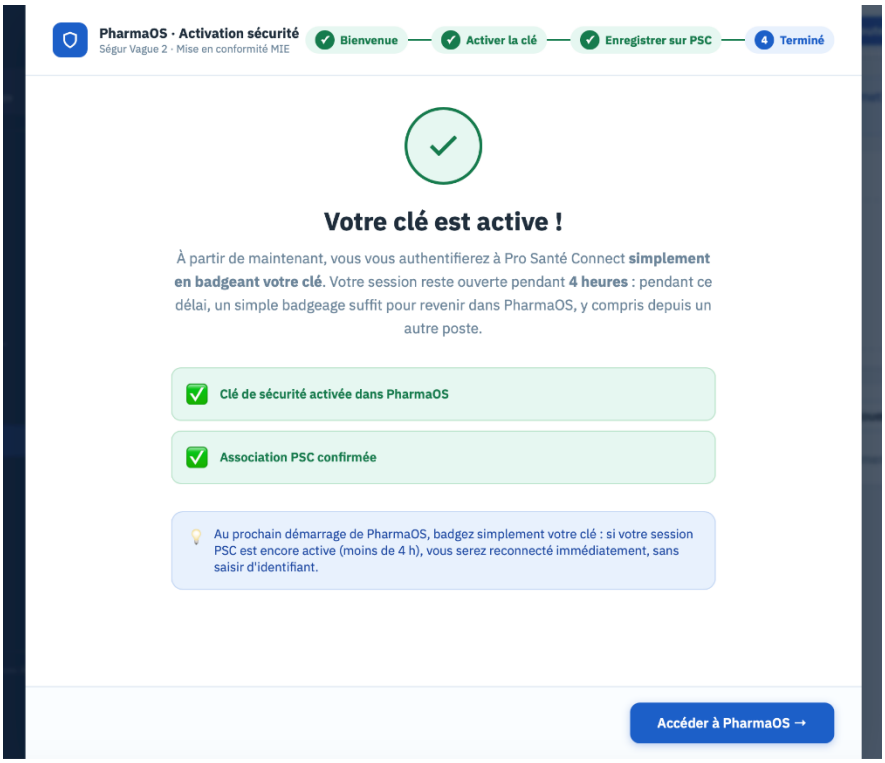


Il est recommandé à cette étape de proposer à l'utilisateur une validation du rapprochement de son identité Pro Santé Connect avec son identité LGO.

Etape 5 : Une fois authentifié, le LGO lance l'ouverture de la page d'enregistrement d'une clé de sécurité sur Pro Santé Connect : l'utilisateur enregistre alors sa clé comme moyen d'authentification Pro Santé Connect



Etape 6 : La clé de sécurité est enregistrée sur Pro Santé Connect, l'utilisateur est de retour dans son LGO : sa clé de sécurité est désormais son moyen d'authentification Pro Santé Connect, et son 1FA pour l'usage en itinérance.



Les modalités d'intégration détaillées, ainsi que les spécifications des flux associés (authentification, gestion de session, appels aux services), sont précisées dans les guides techniques Pro Santé Connect mis à disposition des éditeurs et feront l'objet d'un accompagnement spécifique auprès des éditeurs.

Ces guides couvrent notamment :

- l'intégration des mécanismes d'authentification forte (2FA) ;
- la gestion des sessions et des usages en environnement nomade ;
- les modalités d'utilisation des moyens d'identification électronique (clés de sécurité), selon les technologies retenues (WebAuthn, DESFire, etc.).

3.2.5.5 Rappels réglementaires sur l'identification électronique

- Référentiel d'identification électronique, rendu opposable par l'arrêté du 28/03/2022 intégrant notamment l'obligation de l'implémentation de Pro Santé Connect pour les services numériques sensibles
- Référentiel Pro Santé Connect, rendu opposable par l'arrêté du 4/04/2022
- 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

3.2.5.6 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 architecture « 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.

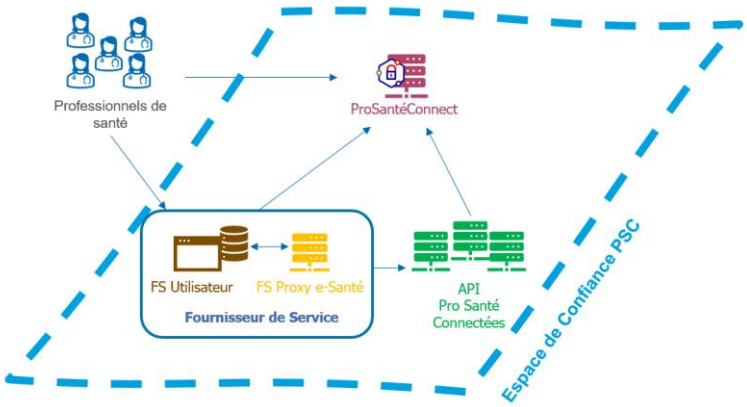


Schéma simplifié de l'Espace De Confiance (FS Proxy e-santé et FS Utilisateur)

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, y compris en mobilité entre postes (session nomade). Les modalités d'intégration sont précisées dans les guides d'intégration de la session nomade et la documentation technique Pro Santé Connect.

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.

3.2.5.7 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-PHA-LGO-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 fournisseurs de données Exigences de l'espace de confiance Pro Santé 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 – Officines	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	Parcours de raccordement à l'espace de confiance PSC	

3.2.6 Conformité aux téléservices

3.2.6.1 Objectifs pour le LGC en vague 2 :

Pour la gestion de l'appli carte Vitale, de l'ordonnance numérique ainsi que pour l' INSi et DMP, un LGC en vague 2 doit être conforme aux spécifications d'intégration de chacun de ces téléservices dématérialisés de l'Assurance Maladie.

La conformité aux spécifications d'intégration de ces téléservices est validé par le Centre National d'Agrément (CNDA).

3.2.6.2 Fonctionnalités couvertes par les exigences vague 2

	Conformité aux téléservices	Exigences associées
6.1	**Gestion de l'application carte vitale**	
	• Agrément au Cahier des Charges SESAM-Vitale 1.40 Addendum 8 (ou plus) pour l'intégration de l'application Carte Vitale.	SC.APCV.01
6.2	**Gestion de l'ordonnance numérique**	
	• Agrément au cahier des charges « Guide d'intégration Ordonnance numérique Pharmaciens » de la CNAM en authentification directe par CPS et par API PSC. • Homologation CNDA pour intégrer l'Ordonnance Numérique par API Pro Santé Connectée.	LGO.ON/CONF.07 LGO.ON/PSC.61
6.3	**DMP**	
	• Homologué CNDA conformément au Guide d'intégration DMP pour l'alimentation en authentification indirecte • Homologué CNDA pour le profil consultation et alimentation avec le mode Espace de Confiance API PSC	SC.DMP/CONF.22 SC.DMP/PSC.40

Les exigences de conformité aux spécifications d'intégration de ces téléservices complètent les exigences fonctionnelles relatives à ces téléservices.

- Par exemple, l'exigence SC.DMP/PSC.40 de conformité aux spécifications du guide d'intégration DMP complète les exigences fonctionnelles de consultation et alimentation du DMP.
  - Dans ce cadre notamment, il est rappelé que les accès CPx doivent également être pris en compte par les LGO, comme prévu dans le GI DMP
- Dans la même logique, les accès CPx doivent également être pris en compte par les LGO pour l'ordonnance numérique, comme prévu dans le GI ON

En regroupant les exigences de conformité aux spécifications d'intégration d'un téléservice, le candidat au référencement vague 2 aura la possibilité de déposer et valider par l'Agence du Numérique en Santé les preuves de conformité aux exigences fonctionnelles relatives à un téléservice sans attendre la validation par le CNDA de la conformité aux spécifications d'intégration du téléservice[2].

[2] Pour plus de précisions : voir 4.4

Les exigences de conformité au téléservices regroupés dans ce chapitre sont validées indépendamment des unes des autres par l'Agence du Numérique en Santé.

3.2.6.3 Présentation détaillée des principales évolutions

Optimisation des transactions de consultation du DMP

Afin de répondre aux exigences de détection des nouveautés et des mises à jour documentaires (notamment pour l'information sur les versions récentes), de nouvelles modalités d'implémentation sont définies pour le Ségur Vague 2.

Que la détection s'opère de manière automatique dès l'accès au dossier patient (Médecins) ou lors de l'accès volontaire au DMP (Sages-femmes et Paramédicaux, Officines), l'objectif est double : garantir une information pertinente au professionnel de santé sans action manuelle de recherche, tout en préservant les performances du logiciel et du SI-DMP.

Ces recommandations techniques, qui reposent sur une utilisation optimisée des journaux de soumissions (SubmissionSets) et des liens de remplacement (RPLC), sont officiellement intégrées au Guide d'implémentation DMP (GI DMP 2.10 MCO 3). Pour accompagner les éditeurs, un Guide d'optimisation des transactions de consultation DMP (accessible sur le site de l'ANS à ce lien : https://esante.gouv.fr/sites/default/files/media/document/Guide_optimisation_dmp.pdf) détaille les flux algorithmiques à privilégier pour assurer la fluidité de l'interface utilisateur. Cette approche commune permet d'industrialiser la gestion de l'obsolescence documentaire et la récupération des nouveaux documents tiers, quel que soit le secteur d'activité

Application Carte Vitale (ApCV)

L'application carte Vitale est la version digitale de la carte Vitale qui propose une solution sécurisée et simple d'utilisation pour l'identification et l'authentification des assurés sur ordiphone. Elle est un moyen d'authentification dématérialisé permettant de sécuriser l'accès aux téléservices, aux côtés de la eCPS.

Le système ApCV proposera donc un service de fournisseur d'identités (niveau eIDAS substantiel), permettant un accès sécurisé aux services de la sphère santé sociale (MES, télémédecine, etc.) et aux services accrochés à France Connect.

L'application Carte Vitale est un portefeuille sectoriel de 4 identités :

- L'identité civile, disponible uniquement pour l'utilisateur de l'appli carte Vitale correspond à l'identité pivot transmise par FranceConnect,
- L'identité patient (ou identité INS), disponible pour l'utilisateur et ses bénéficiaires,
- L'identité AMO, disponible pour l'utilisateur et ses bénéficiaires, porte les informations d'identification nécessaire à la prise en charge des soins notamment (NIR, nom, prénom, date de naissance …),
- L'identité AMC pour l'utilisateur et ses bénéficiaires : restant à définir avec les AMC.

Ordonnance numérique

Le service Ordonnance numérique permet de dématérialiser l'ensemble du circuit des prescriptions (médicaments, dispositifs médicaux, biologie médicale, actes infirmiers, …) entre les professionnels de santé et les patients. Côté officine, le LGO assure les fonctions de récupération, d'exécution et de transmission des données associées à la dispensation.

En vague 1, la gestion de l'ordonnance numérique devait être conforme aux Exigences de la CNAM certifiées par le CNDA. Pour la vague 2, le cahier des charges Assurance Maladie V3 est pris en compte avec notamment la création d'un **mode de transmission séquentiel** (mise à jour de la base en temps réel avec les données d'exécution et nouveau service permettant de mettre à jour l'ordonnance numérique post facturation), et les points suivants embarqués :

- Consignes pour **automatiser le rapprochement prescription / délivrance**
- Facilitation du processus **d'intervention pharmaceutique (favoris)**
- **Pharmacien correspondant et Dispensation conditionnelle**
- Précisions sur les simplifications permises par le décret (**Ordo sécurisée sur papier libre**…)

- **Amélioration des tableaux de bord**

3.2.7 Sécurité des SI

3.2.7.1 Objectifs pour le LGO 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 a été élaboré :

- 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 ;

3.2.7.2 Fonctionnalités couvertes par les exigences vague 2

	Sécurité des SI - Fonctionnalités du périmètre Vague 2	Exigences associées
7.1	**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. Intégrer dans le plan d'assurance sécurité du système les mesures de sécurité entre l'hébergeur et la structure utilisatrice, si l'industriel ou un tiers sous sa responsabilité assure l'hébergement des composants du système	SC.SSI/GEN.01 SC.SSI/GEN.02.BIS SC.SSI/GEN.11 SC.SSI/GEN.20 SC.SSI/GEN.03.BIS
7.2	**Gestion des comptes, des permissions et des sessions des administrateurs et des utilisateurs**	
	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.	SC.SSI/IAM.92
	Sécurisation des processus de gestion des attributs d'identité, tant lors de la création que de la modification des attributs d'identité.	SC.SSI/IE.33
	Renforcement de la sécurité des comptes, notamment lors de la déconnexion des systèmes.	SC.SSI/IE.38
7.3	**Gestion des sauvegardes**	
	Elaboration et application d'un processus de sauvegarde et de restauration.	SC.SSI/GEN.21.BIS
7.4	**Production et conservation des 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

3.2.8 Autres fonctionnalités

3.2.8.1 Objectifs pour le LGO en vague 2

Afin de soutenir le déploiement du Ségur numérique en pharmacie d'officine et d'assurer un suivi efficace de la qualité des données de santé, la vague 2 introduit pour le LGO les fonctionnalités suivantes :

- La production d'un tableau de bord permettant au pharmacien de suivre le taux d'identités INS qualifiées au sein de sa file active de patients, contribuant ainsi à l'amélioration continue de l'identitovigilance ;
- L'intégration d'un lien vers la météo des services numériques en santé, permettant au professionnel de visualiser en temps réel l'état des services de l'ANS et de comprendre rapidement les indisponibilités éventuelles.

3.2.8.2 Fonctionnalités couvertes par les exigences vague 2

Autres fonctionnalités – Fonctionnalités du périmètre Vague 2		Exigences associées
8.1	**Production d'indicateurs**	
	Production d'un tableau de bord présentant le taux d'identités INS par statut	TBB.INS.01
8.2	**Suivi des services ANS en temps réel**	
	Intégration d'un lien vers la météo des services ANS	SC.STATPP.01

3.2.9 Dossier Pharmaceutique (DP)

3.2.9.1 Objectifs pour le LGO en vague 2

Les 5 exigences inscrites dans le REM Vague 2 Officine ont pour vocation de faciliter les échanges et l'utilisation du DP à partir du LGO. Elles permettent :

1. De confirmer la mise en place de l'opt-out du DP (exigence de la vague 1 rendue obligatoire).
2. De renforcer la traçabilité du numéro de lot jusqu'au DP des patients.
3. D'accéder au DP sans la carte vitale du patient.
4. De s'authentifier de manière indirecte par certificat et non via la carte CPS.
5. D'accéder rapidement aux informations de rupture d'approvisionnement des médicaments (DP rupture).

3.2.9.2 Fonctionnalités couvertes par les exigences vague 2 :

	Dossier Pharmaceutique – fonctionnalités du périmètre Vague 2	Exigences associées
9.1	Recueil des coordonnées du patient dans le LGO pour gérer l'opt-out du DP	LGO/DP.01
9.2	Transmission depuis le LGO vers le DP des N° de lot et de la date de péremption des médicaments dispensés au patient. Accès de l'utilisateur à ces informations pour chaque médicament de l'historique médicamenteux.	LGO/DP.02
9.3	Consultation et alimentation du DP d'un patient dès lors que son identité numérique (INS qualifiée) est déjà connue par le logiciel.	LGO/DP.03
9.4	Connexion au DP par certificat logiciel de personne morale depuis le LGO (et non pas via API PSC).	LGO/DP.04
9.5	Exigence d'ergonomie afin de simplifier l'accès aux informations de rupture d'approvisionnement des médicaments (6 clics à date).	LGO/DP.05

3.2.9.3 A propos du DP

Le DP est à l'articulation des axes d'amélioration bien identifiés dans la lutte contre la iatrogénie : « mieux connaître », « mieux éduquer », « mieux informer » et « mieux organiser ».

Le pharmacien a l'obligation légale d'alimenter le DP à l'occasion de la dispensation de médicaments (art. L1111-23 du code de la santé publique), prescrits ou non, sauf en cas d'opposition du patient. Celui-ci peut aussi s'opposer à consultation de son DP.

A l'officine, l'accès au DP-Patient se fait via le logiciel de gestion d'officine (LGO).

Avec la parution du décret du 3 avril 2023, tout bénéficiaire de l'assurance maladie disposera d'un DP automatiquement ouvert sauf opposition de sa part. La consultation du DP par le pharmacien permet de visualiser les médicaments dispensés (remboursés ou non, prescrits ou non) au cours des 12 derniers mois (3 ans pour les médicaments biologiques et 21 ans pour les vaccins).

Le REM permet à l'éditeur d'identifier les évolutions essentielles nécessaires pour permettre le référencement du LGO conformément aux exigences relatives au DP du dossier de spécifications de référencement (DSR) officines (ex : accès sans carte vitale si INS qualifiée, authentification via un certificat logiciel de personne morale et non pas avec la carte CPS…).

3.2.10 Remontée automatique des documents médicaux par MSSanté

3.2.10.1 Objectifs pour le LGO en vague 2

Le dispositif vise à faciliter l'alimentation en documents de santé à des fins de suivi épidémiologique et de dépistage. Il a pour objectif de permettre aux professionnels de santé de se conformer à leurs obligations réglementaires de transmission sans avoir à effectuer de double saisie, en opérant directement depuis leur logiciel métier.

Ce mécanisme de remontée automatique des documents est strictement encadré :

- Finalité et Déclenchement : La remontée des documents est activée uniquement en cas de besoin de suivi épidémiologique (par exemple en cas de crise sanitaire) ou pour des obligations permanentes (comme les certificats de santé de l'enfant ou les maladies à déclaration obligatoire).
- Cadre Légal : L'activation de ces envois est toujours conditionnée à un cadre réglementaire strict. Chaque règle de remontée ("Trigger") fait l'objet d'un projet dédié et aucune ligne n'est ajoutée sans justification juridique.
- Mise en œuvre : L'envoi est déclenché automatiquement lorsqu'un effecteur produit un document correspondant aux règles nationales (type de document, période, etc.), via la Messagerie Sécurisée de Santé (MSS).
- Garanties : Le dispositif intègre des garanties de gouvernance (avec représentants des PS et patients) , de transparence (le fichier de règles est public et non modifiable) , et des mesures de protection des données (pseudonymisation irréversible et absence de stockage des documents au niveau du Concentrateur).

3.2.10.2 Fonctionnalités couvertes par les exigences vague 2

Suivi épidémiologique– Fonctionnalités		Exigences associées
10.1	**Fichier trigger**	
	Télécharger quotidiennement le fichier de règles ("trigger") depuis une URL paramétrable. Vérifier sa signature électronique à l'aide du certificat IGC Santé. Mettre à jour (initialiser, annuler et remplacer) automatiquement les règles de remontée des documents médicaux sans validation utilisateur. Tracer systématiquement la récupération du fichier, la vérification de sa signature et la mise à jour des règles.	SC.TRI.01
10.2	**Envoi d'un document de santé correspondant aux règles du fichier trigger**	
	Transmettre automatiquement par messagerie sécurisée les documents validés et conformes aux règles de remontée. Recueillir et tracer le consentement ou le refus du patient pour la remontée du document lorsque les règles l'exigent.	SC.TRI.02 SC.TRI.03 SC.TRI.05

	Permettre la saisie de ce consentement par l'utilisateur si nécessaire et afficher le message d'information correspondant. Tracer l'ensemble de l'opération, incluant l'identité du patient, le type de consentement et les détails du document.	

3.2.11 Exigences issues de la vague 1 LGO

3.2.11.1 Rappel des objectifs pour le LGO en vague 1

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

- La génération de certains types de documents et données numériques, et notamment la note de vaccination ;
- 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/Mon espace santé du patient ;
- L'intégration des documents et données numériques reçus de professionnels de santé par MSSanté ou provenant du DMP/Mon espace santé patient ;
- La conformité aux référentiels et services socles du numérique en santé (INS, DMP-Compatibilité, MSSanté, Pro Santé Connect, ApCV, ePrescription numérique) ;

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

3.2.11.2 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/va1.08 INS/va1.15 INS/va1.20 INS/va1.21 INS/va1.22 INS/va1.23 INS/va1.25 INS/va1.27 INS/va1.32 INS/va1.36 INS/va1.37 INS/va1.44 INS/va1.47 INS/va1.48 INS/va1.50 INS/va1.51 INS/va1.52 INS/va1.53 INS/va1.54 INS/va1.56 INS/va1.60**
Gestion et partage des documents de santé	**Production des documents au format CDA R2 conformes au CI-SIS**	**DOC/va1.01 DOC/va1.05**
	Génération du document	**LGO.DOC/va1.02**
	Insertion de contenu dans le document	**LGO.DOC/va1.03 LGO.DOC/va1.04**
	Génération de la note de vaccination	**LGO.DOC/va1.06**
	Affichage d'un document entrant	**LGO.DOC/va1.07**

Consultation et alimentation du DMP / Mon espace santé	**Alimentation systématique de Mon espace santé**	**DMP/va1.01**
	Consultation du webPS DMP par appel contextuel	**DMP/va1.02**
	Paramétrage des données de masquage et de l'opposition à l'envoi au DMP	**DMP/va1.17**
	Authentification (alimentation du DMP)	**LGO.DMP/va1.02**
Gestion de la MSSanté	**Envoi de messages et de documents CDA R2 par MSSanté**	**MSS/va1.08 MSS/va1.11 MSS/va1.12 MSS/va1.13 MSS/va1.14 MSS/va1.15 MSS/va1.16 MSS/va1.20 MSS/va1.22 MSS/va1.40**
	Transmission du document au PS	**MSS/va1.26**
	Intégration de l'annuaire santé	**ANN/va1.01 ANN/va1.02 ANN/va1.03 ANN/va1.04**
Dossier Pharmaceutique	**Accès au contenu et traces du DP**	**DP/va1.02**
	Consultation automatique	**DP/va1.03**
	DP Compatibilité	**DP/va1.04**
	Rappels de lots	**DP/va1.05**
	Ruptures d'approvisionnement	**DP/va1.06**
Autres fonctionnalités	**Portabilité des données**	**PORT/va1.01**
	Tableau de bord services socles — Nombre d'alimentation DMP et d'envoi MSS	**LGO.TBB/va1.01**
	Tableau de bord services socles — Nombre de consultation e-prescription	**LGO.TBB/va1.04**
Ordonnance numérique	**Consultation et exécution d'une e-Prescription — Ergonomie**	**LGO.ePresc/va1.04**

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-PHA-LGO-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.

Si une Solution logicielle est commercialisée sous différentes dénominations commerciales, l'Editeur les précise dans sa candidature.

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-PHA-LGO-Va2.

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

Cas des solutions déjà référencées pour un dispositif Ségur

Si la Solution logicielle candidate a déjà fait l'objet d'un référencement pour le dispositif Ségur LGO vague 1, alors le dépôt des preuves du périmètre vague 1 déjà validées n'est pas exigé.

***A noter** : si l'Editeur déclare plusieurs dénominations commerciales et/ou un changement de composant additionnel, les procédures d'habilitation correspondantes auprès du guichet EDC PSC de l'ANS et d'homologation auprès du CNDA, peuvent, selon les cas, être requises.*

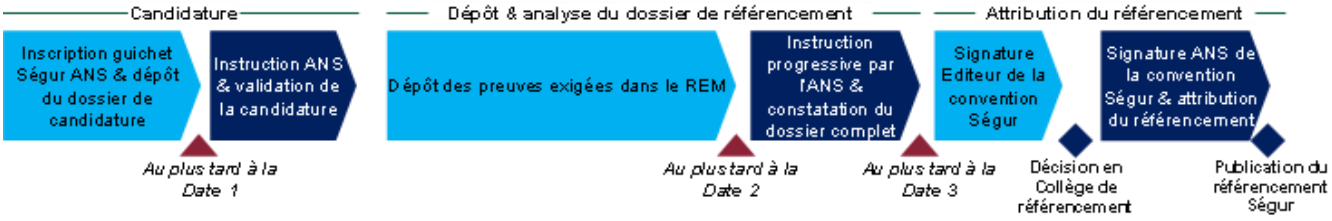
Afin de prendre connaissance des conditions qui s'appliquent à chaque configuration, l'Editeur est invité à consulter la Notice explicative sur l'équivalence des preuves disponible sur le site internet de l'ANS à la date de publication de l'arrêté.

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

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 [3], qui nécessite l'enregistrement préalable au fournisseur d'identité « Industriels Santé Connect » (iSC[4]). Depuis la page d'accueil du Portail des Entreprises du Numérique en Santé :

- **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 Espace de confiance 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 :

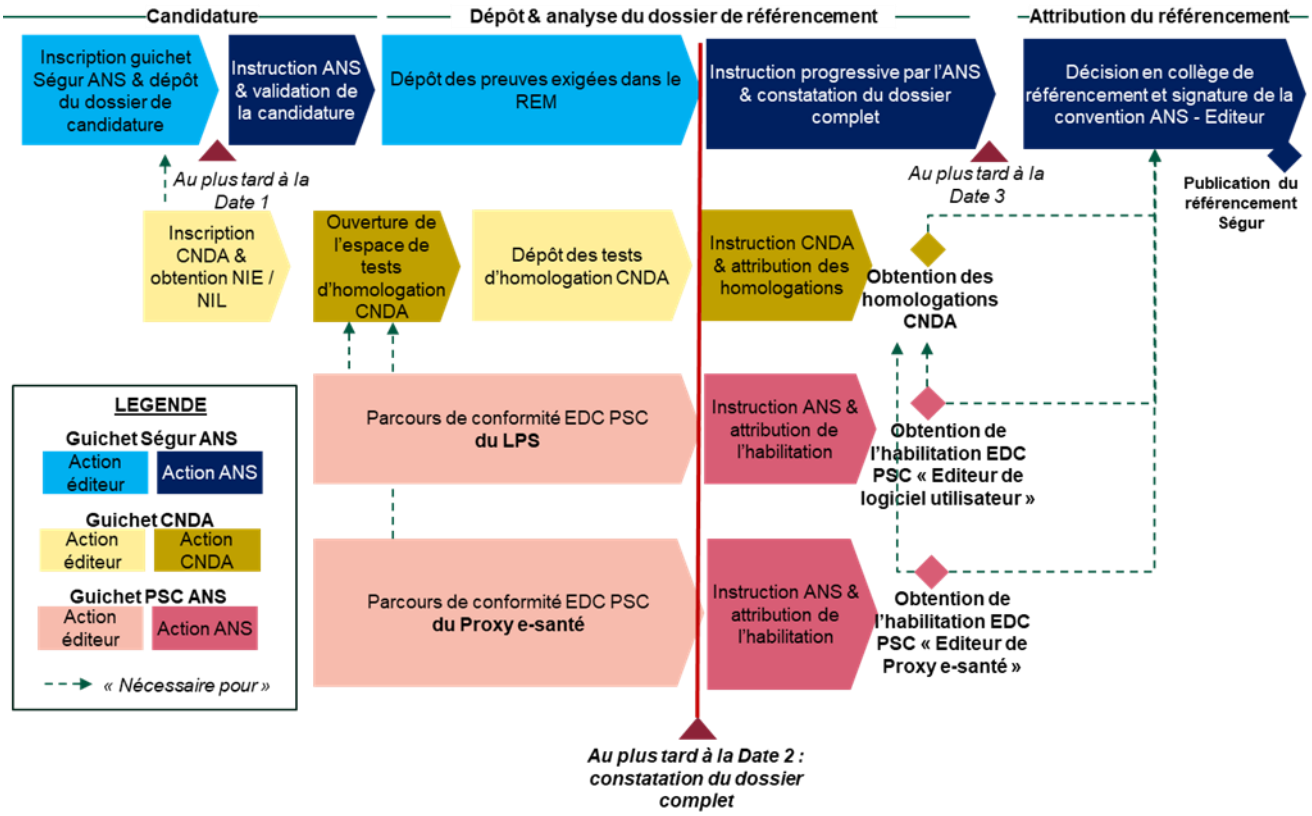
- **Auprès du guichet Espace de confiance Pro Santé Connect (EDC PSC) de l'ANS, accessible sur la plateforme Convergence, l'habilitation « Editeur de logiciel utilisateur »**, selon les dispositions du référentiel PSC, et qui implique notamment :
  - La complétion des chapitres d'exigences de l'espace de dépôt de preuves de ce guichet, correspondant aux exigences présentées dans le document de conformité (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 (EDC PSC) de l'ANS, accessible sur la plateforme Convergence, 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 guichet, correspondant aux exigences présentées dans le document de conformité (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 ;

[3] Voir les CGU disponibles sur https://esante.gouv.fr/ens/user/cgu

[4] Voir les CGU disponibles sur https://isconnect.esante.gouv.fr/enrollement/account/cgu

- 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 sur le guichet d'habilitation EDC PSC, définis par l'ANS ;**
- La décision finale d'homologation du CNDA nécessite d'avoir obtenu au préalable les habilitations EDC PSC 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 son concours, conformément aux instructions qui lui 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 PHA-LGO-Va2

Le système ouvert et non sélectif (SONS) pour PHA-LGO-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 PHA-LGO-Va2
Mercredi 28 avril 2027, 12h00, ci-après **Date 1**	**REFERENCEMENT : Date limite de dépôt du dossier administratif à l'ANS.**
Mercredi 19 janvier 2028, 12h00, ci-après **Date 2**	**REFERENCEMENT** : Date limite de dépôt d'un dossier complet de preuves de conformité
Mercredi 19 avril 2028, 12h00, ci-après **Date 3**	**REFERENCEMENT :** Date de fin des échanges entre l'Editeur et l'ANS pour validation du dossier de preuves
Mercredi 12 juillet 2028, 12h00, 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 14 février 2029, ci-après **Date 5**	**FINANCEMENT :** Fin de la période de réalisation des Prestations Ségur 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 Ségur, selon les modalités présentées à la Section 6.4.
Mercredi 14 mai 2029, 12h00, ci-après **Date 6**	**FINANCEMENT :** Fin de la période de réception des demandes de paiement du solde de la Prestation Ségur. 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 dispositions 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 10 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(s) commerciale(s) (*)

Attention : Les dénominations commerciales déclarées doivent être identiques aux dénominations commerciales déclarées sur le guichet EDC PSC Editeur de logiciel utilisateur ainsi qu'au CNDA.

- Date prévisionnelle du dépôt de dossier de preuves complet.
- Si la Solution logicielle ou a minima son composant principal est déjà référencé pour le dispositif Ségur en vague 1 : le numéro unique de référencement précédemment obtenu ;
- 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.

Attestation sur l'honneur :

L'éditeur doit fournir une attestation lorsque :

- Plusieurs dénominations commerciales sont déclarées pour la Solution logicielle candidate : l'attestation doit confirmer que ces dénominations renvoient à une même Solution logicielle ;
- La Solution logicielle a déjà été référencée sous une autre dénomination commerciale : l'attestation doit confirmer qu'il s'agit de la même Solution logicielle que celle précédemment référencée ;
- Le composant principal de la Solution logicielle candidate est identique à celui d'une Solution logicielle référencée mais un ou plusieurs composants additionnels sont différents.

L'éditeur doit obligatoirement utiliser le modèle d'attestation mis à disposition sur le site Internet de l'ANS. Aucune autre forme d'attestation ne sera acceptée.

Informations CNDA[5] :

- Numéro d'Identification Editeur (NIE délivré par le CNDA) (*).
- Pour chaque dénomination commerciale, Numéro d'Identification Logiciel (NIL délivré par le CNDA) (*).

Informations sur la Solution logicielle :

- Numéro de version technique soumise au référencement pour chaque dénomination commerciale (*).
- Numéro unique de candidature au guichet Espace de confiance Pro Santé Connect Editeur de Logiciel utilisateur (*).
- Pour les Solutions logicielles pour lesquelles l'Editeur entend mobiliser des financements Ségur au titre de l'AF-PHA-LGO-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-PHA-LGO-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.

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.

Composant Proxy e-santé : l'Editeur doit déclarer les éléments relatifs au Composant Proxy e-santé partie de la Solution logicielle.

Composants additionnels (*) : l'Editeur 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 ;
- La présence ou non du composant additionnel dans le référencement précédemment obtenu (cf. informations relatives à la version candidate) ;
- 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-PHA-LGO-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

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

même Exigence (capture d'écrans, vidéos, fichiers, logs, homologations…). Chaque preuve demandée sur la plateforme Convergence est obligatoire.

- Pour chaque homologation à obtenir auprès du CNDA : l'attestation d'homologation, ou à défaut le dépôt au CNDA de l'ensemble des éléments attendus du dossier de l'homologation concernée, tel qu'attesté par le 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 10 jours 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 des conditions définies précédemment relatives à la **Date 3,** transmettre à l'ANS le **compte-rendu de pré-examen déclenchant une date d'examen** (via une copie d'écran de son espace personnel CNDA). L'attestation d'homologation pourra être fournie au-delà de la Date 3. Elle reste obligatoire pour l'obtention du référencement Ségur.
- 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. La 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
CDA R2	Clinical Document Architecture, Release 2.0, standard de dématérialisation des documents médicaux électroniques exploitant la syntaxe XML (N1 : données non structurées, N3 : données structurées)
CI-SIS	Cadre d'Interopérabilité des Systèmes d'Information de Santé
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
DP	Dossier Pharmaceutique
FIDO2	Fast IDentity Online 2, standard ouvert d'authentification sans mot de passe porté par l'Alliance FIDO
INS	Identité nationale de santé
LGO	Logiciel de Gestion d'Officine
LPS	Logiciel de Professionnel de Santé
MES	Mon espace santé
MIE	Moyen d'Identification Electronique
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
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
NFC	Near Field Communication — technologie de lecture sans contact
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
PSC	Pro Santé Connect est un fédérateur de fournisseurs d'identité au standard OpenID. Pro Santé Connect permet aux professionnels de s'authentifier avec une e-CPS (application mobile), une carte CPS physique, ou une clé de sécurité de type MIE FIDO2 à tous les services numériques de santé raccordés à Pro Santé Connect