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

AGENCE
DU NUMÉRIQUE
EN SANTÉ

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

DOSSIER PATIENT INFORMATISE (DPI)
VAGUE 2

Dossier de spécifications de référencement (DSR)

DSR-HOP-DPI-Va2
Annexe II à l'arrêté relatif à un programme de financement destiné à encourager l'équipement numérique des structures hospitalières - Fonction « Dossier patient informatisé » Vague 2
Version mise à jour suite à arrêté modificatif – mars 2025

Financé par
l'Union européenne
NextGenerationEU

SÉGUR NUMÉRIQUE
LA E-SANTÉ FRANÇAISE

Historique du document – suivi des modifications apportées			
Version	Date	Auteur	Commentaires / modifications
V1	*20/05/2024*	*ANS*	*Version publiée sur le site de l'ANS et référencée dans l'arrêté du 16 mai 2024*
V1.1	*10/12/2024*	*ANS*	*Mise en cohérence avec le REM concernant le « consentement » suite à la décision du Conseil Constitutionnel n° 2024-1101 QPC du 12 septembre 2024*
V1.2	14/03/2025	ANS	Version mise à jour suite à publication de l'arrêté du 14 mars 2025 : ▪ Section 4.1 : mise à jour du calendrier réglementaire du SONS Afin de faciliter la lecture, les modifications apportées sont surlignées.
V1.2b	*25/04/2025*	*ANS*	*Rétablissement des éléments relatifs au consentement suite à une anomalie du document, §3.2.2*

Sommaire

1 PRESENTATION ET DEFINITIONS 4
1.1 Présentation du dispositif SONS HOP-DPI-Va2 4
1.2 Définitions 4
2 PERIMETRE LOGICIEL ELIGIBLE AU REFERENCEMENT 6
3 EXIGENCES LOGICIELLES 7
3.1 Formalisme de description et règles d'application des Exigences 7
3.2 Présentation des Exigences logicielles HOP-DPI-Va2 8
3.2.1 Gestion et partage des documents de santé 8
3.2.2 Consultation et alimentation du DMP / Mon espace santé 12
3.2.4 Gestion de la MSSanté 20
3.2.5 Identification électronique & ProSanté Connect 23
3.2.6 Sécurité des SI 24
3.2.7 Production d'indicateurs 26
3.2.8 Exigences issues de la vague 1 DPI 28
4 MODALITES DE REFERENCEMENT De la Solution logicielle 30
4.1 Calendrier du SONS HOP-DPI-Va2 30
4.2 Principes de Référencement 31
4.2.1 Solution logicielle éligible au référencement 31
4.2.2 Contrôles des Exigences 31
4.2.3 Audits de conformité 31
4.2.4 Publicité des informations 32
4.2 Dépôt et validation du dossier administratif 32
4.3 Dépôt de dossier complet de preuves de conformité 34
4.4 Instruction du dossier de preuves 34
4.5 Signature de la convention Ségur par l'Editeur et attribution du référencement 35
4.6 Espace Authentifié, Support et FAQ 36
4.7 Confidentialité 37
4.8 Protection des données à caractère personnel 37
4.9 Convention de preuve 38
5 GLOSSAIRE 39

1 PRESENTATION ET DEFINITIONS

1.1 Présentation du dispositif SONS HOP-DPI-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 « Dossier Patient Informatisé » (DPI) des établissements de santé est encadré par l'arrêté du ministre délégué auprès de la ministre du travail, de la santé et des solidarités, chargé de la santé et de la prévention, 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-HOP-DPI-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-HOP-DPI-Va2 (présent document)**, qui présente les modalités de présentation et d'instruction des demandes de référencement ;
- **Le document d'appel à financement AF-HOP-DPI-Va2,** qui définit l'ensemble des règles et conditions associées à l'attribution et au versement des financements, ainsi que les modalités de présentation et d'instruction des demandes de financement et de paiement.

1.2 Définitions

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

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

Client : le Client désigne l'Etablissement de santé ou le groupe d'établissements 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 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 des dossiers administratifs, 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. L'accès auxdites informations se fait au travers d'un compte nominatif créé via ISC.

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

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

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

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

Solution logicielle : une solution logicielle est constituée d'un composant unique, ou d'un Composant principal et 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 le composant unique, ou le Composant principal et les 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 PERIMETRE LOGICIEL ELIGIBLE AU REFERENCEMENT

Le référencement HOP-DPI-Va2 concerne la fonction « Dossier Patient Informatisé » (DPI) des établissements de santé, qui a vocation à stocker l'ensemble des documents liés au parcours de soins du patient au sein de l'établissement. Il contient donc les différents documents devant alimenter le DMP et être transmis via MSSanté et plus largement l'ensemble des documents nécessaires à la bonne prise en charge du patient par l'établissement (NB : il ne s'agit pas des logiciels de spécialités).

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

- Gérer les informations nécessaires et utiles à la prise en charge et au suivi du patient, à la traçabilité des soins et actions entreprises.
- Gérer les diverses informations médicales concernant le patient, antérieures à l'hospitalisation ou produites au cours du séjour en établissement, telles qu'observations, lettres de liaison de sortie, comptes rendus opératoires, ordonnances, comptes rendus d'examens, etc.
- Faciliter la production de documents médicaux tels que la lettre de liaison de sortie, le compte rendu opératoire, les ordonnances.
- Permettre la consultation des documents du DMP / Mon espace santé.
- Implémenter des profils IHE et des transactions HL7 afin d'être interopérables avec le reste du système d'information hospitalier.

Pour information, un dispositif HOP-PFI-Va2, distinct du présent dispositif, concerne la fonction « Plateforme d'intermédiation » (PFI) des établissements de santé, qui assure l'échange et le partage sécurisé des documents à l'extérieur du SIH, via la MSSanté et le DMP. En fonction du périmètre fonctionnel couvert, une même Solution logicielle peut présenter sa candidature au référencement HOP-DPI-Va2 d'une part, et au référencement HOP-PFI-Va2 d'autre part.

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-HOP-DPI-Va2.**

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

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

Profils applicables à la solution candidate au référencement

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

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

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

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

Pour le REM-HOP-DPI-Va2, le seul Profil optionnel, intitulé « Authentification PSC par CIBA », regroupe les Exigences qui ne s'appliquent que lorsque l'Editeur a choisi d'implémenter dans sa Solution logicielle l'authentification ProSanté Connect par le protocole CIBA.

Profil	Critère(s) de choix des Profils *(Profil à sélectionner par l'Editeur dans les cas suivants)*
Général	N/A (Profil imposé à toutes les solutions candidates au référencement)
Authentification PSC par CIBA	Obligatoire dès lors que l'Editeur a choisi d'implémenter dans sa solution l'authentification PSC par CIBA

Cas des solutions déjà référencées en vague 1

Dans le REM-HOP-DPI-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 ;
- Certaines Exigences de la vague 1 qui relevaient d'un Profil optionnel sont désormais imposées à toute Solution candidate ;
- Certains Profils de la vague 1 peuvent être exigés en fonction des choix de Profils fait par l'Editeur dans le cadre du présent dispositif.

Pour le REM-HOP-DPI-Va2, les règles sont les suivantes :

- Si la solution candidate est déjà titulaire d'une attestation de référencement au titre du dispositif HOP-DPI-Va1, avec le Profil « Intégration INS », alors le dépôt des preuves des Exigences du Périmètre vague 1 n'est pas exigé.
- Si la solution candidate est déjà titulaire d'une attestation de référencement au titre du dispositif HOP-DPI-Va1, sans le Profil « Intégration INS », alors seul le dépôt des preuves du Périmètre vague 1 correspondant à ce Profil est exigé.

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

3.2 Présentation des Exigences logicielles HOP-DPI-Va2

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

1. **Gestion et partage des documents de santé**
2. **Consultation et alimentation du DMP / Mon espace santé**
    - Information et consentement du patient
    - Consultation du DMP
    - Alimentation du DMP
    - Remise en visibilité des documents du patient
3. **Gestion de la MSSanté**
4. **Identification électronique & ProSanté Connect**
5. **Sécurité des SI**
6. **Production d'indicateurs**
7. **Exigences issues de la vague 1 DPI (périmètre « Vague 1 »)**

3.2.1 Gestion et partage des documents de santé

Objectifs pour le DPI en vague 2 :

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

- Permettre la **visualisation des documents de santé** consultés dans le DMP ou reçus par MSSanté au format CDA en particulier pour l'affichage des métadonnées des documents ou dans le cas des documents au format CDA R2 N3 avec un PDF encapsulé (en première intention visualisation du PDF et si l'utilisateur le demande afficher le document CDA R2 N3 avec une feuille de style).

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

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

- Implémenter le volet du CI-SIS ***Transmission de document(s) CDA en HL7v2***, afin que le DPI puisse transmettre les documents qu'il produit à destination de la fonction PFI chargée d'alimenter le DMP et/ou d'envoyer le(s) document(s) en pièce jointe d'un courrier électronique MSSanté à des destinataires.
- Implémenter le volet du CI-SIS ***Transmission au LPS de documents CDA provenant d'un courriel MSSanté*** afin que le DPI puisse intégrer des courriels MSSanté reçus sur des BAL applicatives et exploitées par la fonction PFI d'un établissement de santé.

Fonctionnalités couvertes par les exigences vague 2 :

N°	GESTION ET PARTAGE DES DOCUMENTS DE SANTE - Fonctionnalités du périmètre Vague 2	Exigences associées
1.1	**Affichage des documents au format CDA R2 N1 et N3**	
	- Mise en visibilité de la copie PDF encapsulée qui doit affichée de préférence lors de l'ouverture pour les documents CDA R2 N3. Possibilité de basculer vers le format CDA R2 N3 via la feuille de style de l'ANS ou du producteur - Affichage des métadonnées des documents CDA R2 N3 et PDF associés sur une seule ligne dans l'espace documentaire	SC.CDA/DD.15 SC.CDA/VISU.03 SC.CDA/INT.15 SC.CDA/VISU.01
1.2	**Production des documents au format CDA R2 conformes au CI-SIS**	
	- Production des documents au format CDA intégrant le datamatrix et marquage 'INS à scanner'	SC.CDA/VISU.04
1.3	**Navigation dans le dossier patient local et identification des documents importés depuis / exporté vers le DMP et la MSSanté**	
	- Identification (sans clic) dans le dossier patient des documents importés depuis le DMP et la MSSanté - Identification dans le dossier patient des documents exportés vers le DMP et la MSSanté - Affichage (sans clic) du statut de l'identité du patient (provisoire, validée, récupérée, qualifiée), au niveau de l'interface "dossier patient" - Tri des documents importés et produits, à minima, selon le type code et la date de l'acte - Absence de blocage de l'interface graphique de l'utilisateur pendant les requêtes au DMP, Pro Sante Connect et l'Annuaire	SC.CDA/INT.04 SC.CDA/INT.08 SC.CDA/INT.17 SC.DMP/HISTO.01 DPI.DMP/UX.10 SC.DMP/UX.11
1.4	**Information de l'existence et visualisation d'une version plus récente d'un document déjà intégré dans le dossier patient**	
	- Notification de l'utilisateur lors de la consultation d'un document au sein du dossier d'un patient si une version plus récente de ce même document est disponible dans le DMP. Accès direct à la dernière version du document et intégration dans son DPI	SC.CDA/DD.05 SC.CDA/VISU.02
1.5	**Eviction des conflits entre documents identiques**	

	Mise en cohérence du contenu des documents produits lors d'un même acte médical (PDF/A-1, CDA R2 N1, CDA R2 N3)	SC.CDA/DD.02
1.6	**Interopérabilité entre le LPS et la fonction PFI en environnement hospitalier**	
	- Mise en œuvre des volets d'interopérabilité entre les fonctions DPI et PFI pour la gestion des documents CDA envoyés (DMP, MSSanté) et reçus (MSSanté) - Gestion des acquittements techniques et métiers de réception d'un document via la fonction PFI - Transmission à la fonction PFI via le flux HL7 V2 les informations d'identification nécessaires à la constitution du jeton VIHF	DPI.CDA/HL7.01 DPI.CDA/HL7.02 DPI.CDA/HL7.04 SC.DMP/CONF.12

Affichage des documents au format CDA R2 N1 et N3

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

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

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

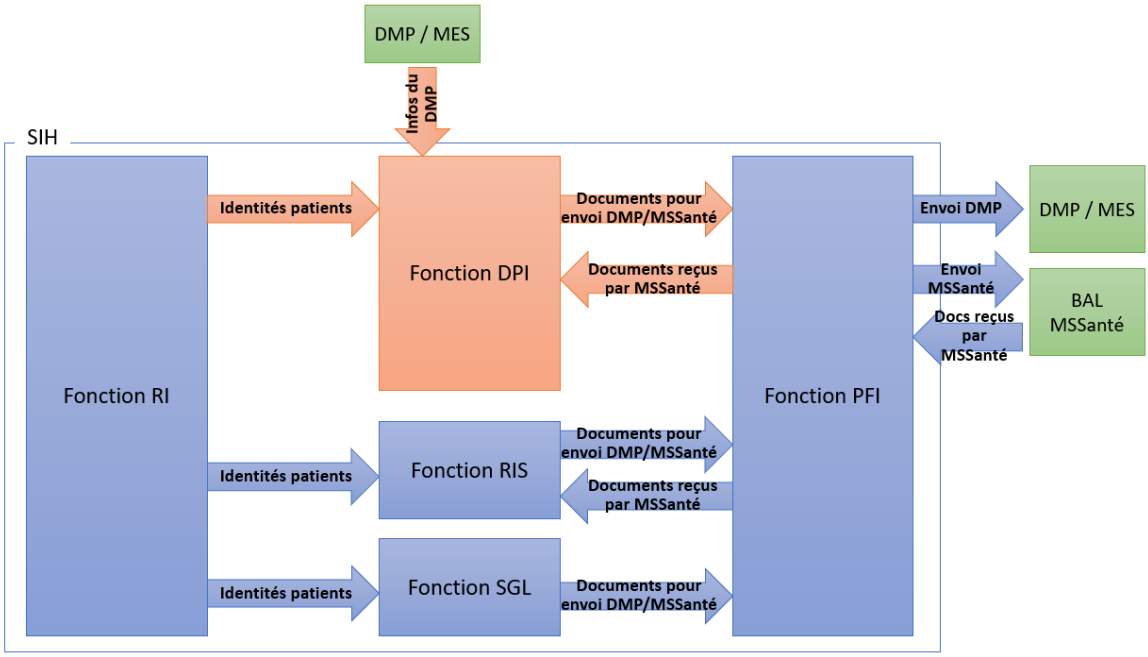
Interopérabilité des fonctions DPI et PFI

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

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

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

Flux d'interopérabilité avec la fonction DPI



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

La gestion des documents de santé doit in fine permettre le partage des documents de santé, conformément aux obligations présentes dans l'article L. 1111-15 du Code de la santé publique. Cet article décrit les **obligations de partage par voie numérique** des « *éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge* » pour les professionnels de santé.

Ce partage s'effectue à deux niveaux :

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

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

Rappel réglementaire : l'Identité Nationale de Santé (INS)

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

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

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

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

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

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

3.2.2 Consultation et alimentation du DMP / Mon espace santé

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

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

a) Information et consentement du patient

Objectifs pour le DPI en vague 2 :

Dans le cadre de l'utilisation du DMP / Mon espace santé, le professionnel de santé a **l'obligation d'informer le patient** de l'alimentation de son espace santé.

- Cette information peut notamment être délivrée par un collaborateur de la structure ou faire l'objet d'une information écrite (par exemple : à la prise de rendez-vous, de la préadmission, à l'accueil, salle d'attente).
- Cette information n'est à donner qu'une seule fois dans le cadre de l'épisode de soin du patient.
- Le patient peut s'opposer à l'alimentation pour motif légitime (la légitimité du motif est à l'appréciation du professionnel).

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, qui doit pouvoir exprimer son opposition à l'alimentation et son consentement à la consultation et conditionner ainsi le comportement du logiciel.

-

- L'alimentation du DMP 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 selon la discussion avec le patient sur le motif légitime,
- La consultation du DMP ne peut se faire que sur consentement explicite du patient, celui-ci peut ne pas consentir sans avoir à le justifier.
- Ces consentements peuvent être renseignés à l'initiation de la prise en charge et doivent être accessibles et modifiables ultérieurement par le professionnel, par exemple en cliquant sur un bouton "Mon espace santé" au sein du dossier patient. 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 consentements du patient est réalisée en amont de la prise en charge du patient par un professionnel habilité, 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 le cadre d'une prise en charge, plusieurs consentements ou recueils de non-opposition peuvent être requis, afin d'en faciliter la gestion pour les professionnels, il est possible de les regrouper dans une interface dédiée.
- Dans les situations d'urgence 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 an amont des soins ou pour des non professionnels de santé.
- L'information et les consentements du patient sont enregistrés et s'appliquent à l'ensemble de l'équipe de soin prenant en charge le patient pendant la durée de l'épisode de soin, et non à la maille individuelle du professionnel.

- L'épisode de soin correspond à la période de prise en charge du patient. Si l'épisode de soin se poursuit après l'expiration de la durée d'autorisation technique à la consultation du DMP (ex : prise en charge au long court), la transaction d'autorisation peut être renouvelée automatiquement sans redemander aux professionnels de retracer le consentement.

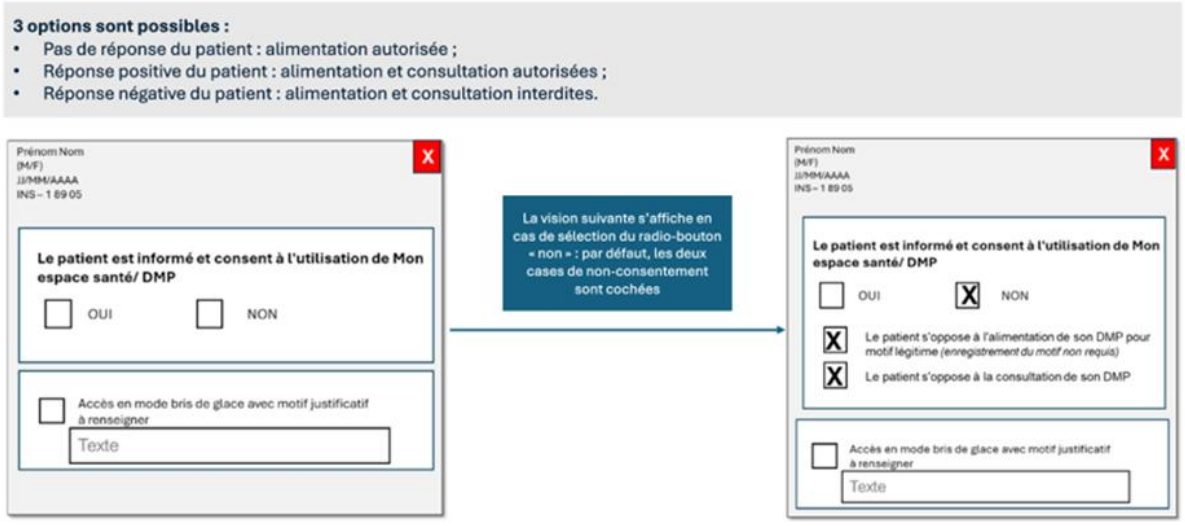
Fonctionnalités couvertes par les exigences vague 2 :

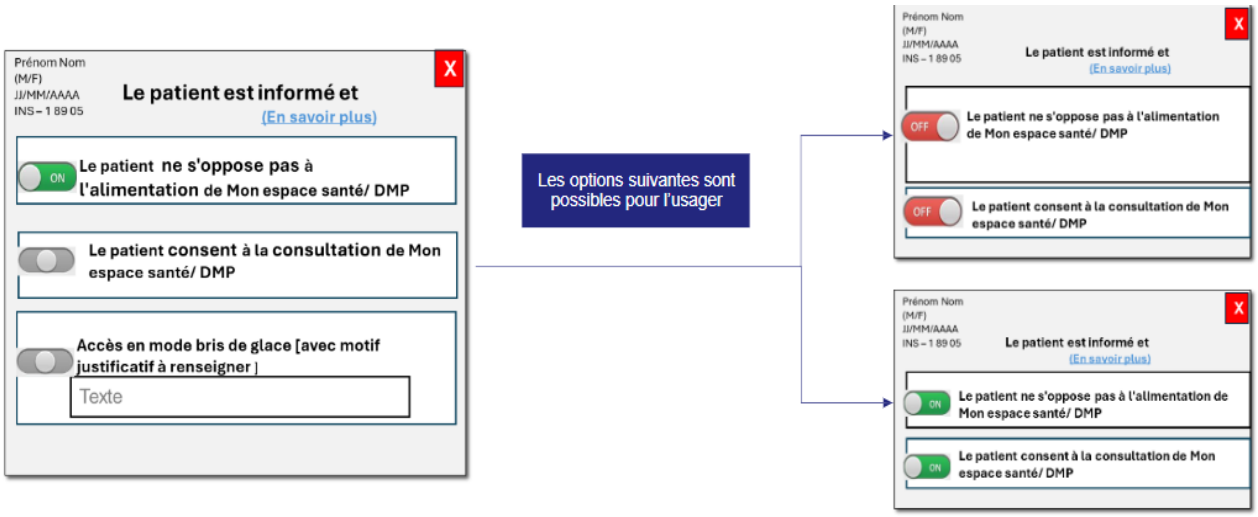
	Information et consentement du patient à l'alimentation et la consultation du DMP / Mon espace santé - Fonctionnalités périmètre Vague 2	Exigences associées
2.1	**Gestion de l'information et du consentement du patient**	
	- Enregistrement et traçage de l'information / la non-information du patient, son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

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

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

Exemple de texte d'information et d'action d'un utilisateur du logiciel métier pour l'information du patient





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

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

b) Consultation du DMP / Mon espace santé

Objectifs pour le DPI en vague 2 :

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

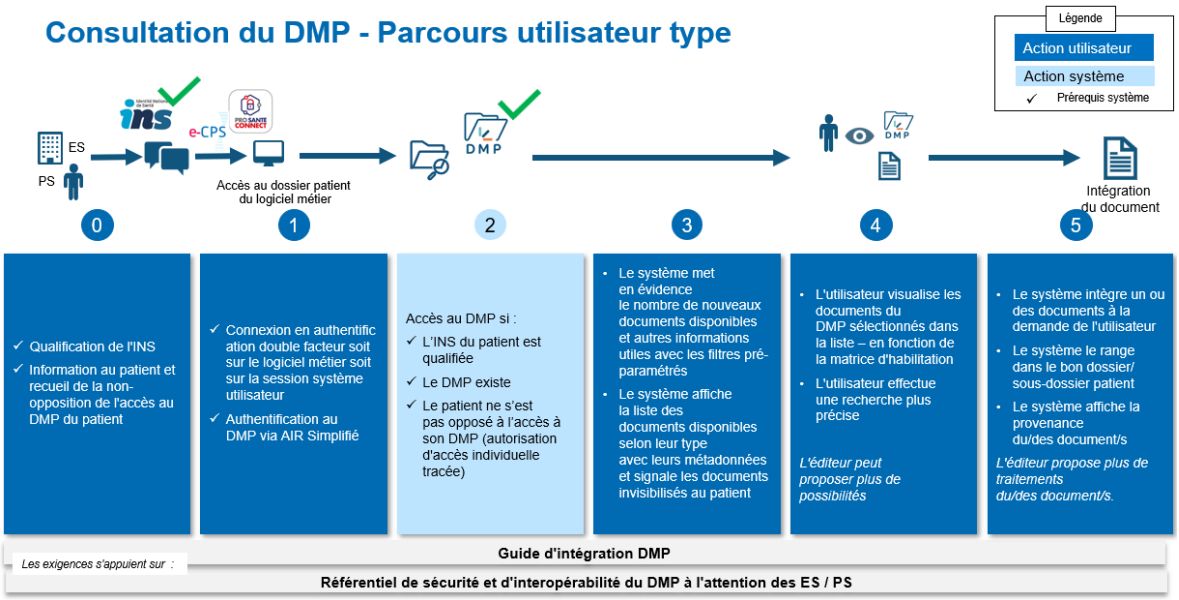
Les objectifs principaux de la vague 2 sont :

- Permettre au professionnel de consulter le profil Mon espace santé du patient **directement depuis son logiciel** (par opposition à l'accès en WebPSDMP et appel contextuel) :
  - Le professionnel **doit savoir sans clic si son patient a un DMP / Mon espace santé ouvert** et si son accès est autorisé.
  - Le professionnel **doit connaître sans clic la provenance et le statut des documents** envoyés et intégrés (provenance, nouvelle version disponible, etc.).
  - Le professionnel **doit disposer facilement du nombre de documents récemment alimentés par des professionnels et structures tiers pour orienter son choix** dans la lecture des documents.
  - Le professionnel doit pouvoir examiner la liste des métadonnées des documents présents dans le DMP afin de pouvoir les visualiser, en mettant en avant les documents invisibles au patient.
  - Le professionnel **peut manuellement intégrer un document de Mon espace santé pour le visualiser** et l'intégrer dans son logiciel.
- Permettre également de consulter le profil Mon espace santé du patient via l'appel contextuel (par mode AIR ou par ProSanté Connect), notamment pour permettre d'accéder à la page de création des notes de vaccination.

NB : Les fonctionnalités de consultation du DMP / MES sont uniquement portées par la fonction DPI et non via la fonction PFI à l'inverse de l'alimentation du DMP, dans le cadre de la vague 2 du Ségur numérique.

Fonctionnalités couvertes par les exigences vague 2 :

	CONSULTATION DE MON ESPACE SANTE - Fonctionnalités périmètre Vague 2	Exigences associées
2.2	**Conformité au référentiel DMP et Information du professionnel sur le contrôle et la traçabilité des accès à Mon espace santé**	
	- Information du professionnel sur le contrôle et la traçabilité des accès au DMP / Mon espace santé via son identifiant national (RPPS) - Trace des accès aux documents provenant du DMP et extraction de ces informations	SC.DMP/CONF.11 SC.DMP/CONF.14 SC.DMP/CONF.15
2.3	**Autorisation de consultation du DMP et information rapide de l'utilisateur sur son contenu**	
	- En cas de consentement du patient, vérification de l'autorisation d'accès au DMP de l'utilisateur authentifié et s'il n'est pas autorisé, positionnement de son autorisation individuelle - Information visible dès l'ouverture du dossier patient de l'existence du DMP du patient et de l'autorisation d'accès de l'utilisateur - Affichage synthétique des documents présents dans le DMP, selon des critères paramétrables par l'utilisateur - Recherche multicritère dans le DMP du patient	SC.DMP/CONF.16 SC.DMP/UX.12 SC.DMP/UX.15 SC.DMP/UX.17 SC.DMP/UX.14 SC.DMP/UX.14.TER SC.DMP/UX.27
2.4	**Intégration de documents du DMP dans le dossier patient local**	
	- Sélection multiple de documents du DMP de la liste présentée et intégration dans le dossier patient	SC.DMP/UX.31
2.5	**Consultation par le mode "AIR" simplifié**	
	- Besoin d'une homologation CNDA pour le profil de consultation avec le mode d'authentification AIR simplifié - Lors d'une transaction, l'identifiant national (RPPS/ADELI) de l'utilisateur est systématiquement transmis	SC.DMP/AIRS.03 SC.DMP/AIRS.06
2.6	**Consultation du webPS DMP par appel contextuel**	
	- Possibilité de consulter le DMP du patient par appel contextuel notamment par ProSanté Connect - Possibilité de consulter le DMP du patient par appel contextuel notamment pari mode AIR Simplifié - Permettre l'accès directement à la note de vaccination via l'appel contextuel	DPI.AUTH.01 DPI.AUTH.02 DPI.DMP/UX.49
2.7	**Accès sécurisé aux images médicales**	
	- Accès à la DRIM Box Consommatrice par appel contextuel depuis le DPI - Accès aux images médicales via le lien présent dans le CR d'imagerie	SC.DB/TRA.04



Détail des actions logicielles pour la consultation du DMP

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

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

Il est impératif que le patient ait été informé de cette action par l'établissement, car le patient reçoit une notification au moment de l'accès à son dossier. Cette information l'informe que le personnel médical pourra avoir accès à son dossier, 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 éventuellement de l'action qu'il a menée pour s'opposer. Si le patient s'est opposé à consultation de son DMP, le logiciel ne lance aucune transaction de consultation et peut afficher cette information (sous forme d'icône) à l'utilisateur connecté.

2. A la première connexion de l'utilisateur à l'interface, le logiciel effectue la requête d'existence du DMP *et* affiche alors l'icône, à côté de l'identité du patient dans le logiciel. Cela permet également de vérifier que l'utilisateur a bien les droits d'autorisation d'accès au DMP. Le logiciel transmet également les informations suivantes.

a. Le FINESS de l'établissement, ayant été enregistré comme autorisé à accéder au DMP

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

b. L'identifiant national du professionnel de santé (RPPS), permettant de vérifier la correspondance et que ce professionnel n'a pas été bloqué par le patient

Une fois que le logiciel a enregistré que le patient a été informé, lorsque l'utilisateur se connecte à l'interface où il pourra avoir les informations du DMP, il est nécessaire que le logiciel positionne automatiquement l'autorisation individuelle d'accès au DMP du professionnel à l'aide de son RPPS (en plus de l'enregistrement du FINESS de l'établissement sur la liste blanche des établissements pouvant avoir accès au DMP via le mode AIR Simplifié). L'autorisation individuelle d'accès permet au DMP de vérifier la correspondance dans le RPPS du professionnel, de vérifier que ce professionnel n'a pas été bloqué par le patient (dans Mon espace santé), tracer cette information dans le DMP et l'afficher au patient. Cette autorisation individuelle à une durée technique de 6 mois dans le DMP. Ainsi, lors des prochaines connexions, il est seulement nécessaire de vérifier son autorisation en même temps que l'existence du DMP.

Le logiciel doit rester fonctionnel lorsque le logiciel effectue les requêtes au DMP.

Si le professionnel n'a pas l'autorisation, alors le logiciel vient positionner automatiquement sans action supplémentaire l'autorisation individuel d'accès technique.

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

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

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

Lorsqu'il y a des documents, le logiciel affiche le nombre de documents versés au DMP du patient depuis un événement paramétrable, sans clic supplémentaire de l'utilisateur.

Les utilisateurs intéressés sont, par défaut, les professionnels de santé et, en priorité, les personnes de leurs équipes ayant la tâche de consolider le dossier médical du patient au sein de l'établissement sanitaire.

Par défaut, le logiciel effectue cette action pour les prises en charge les plus pertinentes, c'est-à-dire pour les patients venus pour des consultations externes ou des urgences. Le logiciel doit compter dans les derniers documents les documents invisibles aux patients et les mettre en visibilité.

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

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

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

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

5. Affichage dans une liste de métadonnées *:* Si l'utilisateur le souhaite (clic), le logiciel affiche dans l'interface "dossier médical", 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).

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

8. 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.

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

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

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

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

Mode Authentification Indirecte Renforcée (AIR) simplifié

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

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

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

NB : En Vague 2 pour les DPI, compte tenu de la mise en œuvre du mode AIR Simplifié, l'implémentation des API Pro Santé Connectées n'est pas imposée. Elle sera néanmoins à envisager dans un proche avenir, comme une fonctionnalité à forte valeur ajoutée pour faciliter l'accès des professionnels à l'ensemble des services Pro Santé Connectés (services socles, Drimbox ...). Afin de préparer les logiciels à ces évolutions, la mise en œuvre de Pro Santé Connect comme moyen d'identification électronique au DPI devient donc obligatoire (conformément à la PGSSI-S), de même que la mise en œuvre d'une fonctionnalité d'accès contextuel au Web PS DMP avec Pro Santé Connect (contexte patient depuis le DPI).

Afin d'offrir une alternative au mode AIR Simplifié, il est également possible de permettre une connexion au DMP avec une authentification directe par carte CPS depuis les logiciels. Ce mode de connexion historique au DMP, éventuellement déjà existant dans certains logiciels, peut bien entendu être maintenu, sans toutefois être imposé dans le cadre de la vague 2.

c) Alimentation du DMP / Mon espace santé

Objectifs pour le DPI en vague 2 :

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

L'objectif de la vague 2 est de :

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

Fonctionnalités couvertes par les exigences vague 2 :

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

Un guide explicatif à destination des établissements de santé sur les modalités techniques, organisationnelles et juridiques de cette reprise d'historique, est mis à disposition sur la page du programme SUN-ES.

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

Objectifs pour le DPI en vague 2 :

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

Ainsi, le logiciel doit alors permettre de :

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

Fonctionnalités couvertes par les exigences vague 2 :

	INVISIBILISATION DE MON ESPACE SANTE - Fonctionnalités périmètre Vague 2	Exigences associées
2.11	Autorisation de consultation du DMP et information rapide de l'utilisateur sur son contenu	
	- Affichage des documents qui sont invisibles au patientet / ou représentants légaux et possibilité de les rendre visible à l'un et/ou à l'autre. - Information directement disponible dans l'interface du « dossier médical » du nombre de documents qui ont été versés au DMP dont les documents invisibles (au patient). - Fonction de recherche et/ou de filtrage basée sur des critères issus des métadonnées XDS du DMP (documents invisibles, période donnée…).	SC.DMP/UX.14.BIS SC.DMP/UX.15 SC.DMP/UX.27

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

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

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

- Un **mode d'envoi par l'acteur de santé auteur du document** (établissement de santé ou laboratoire de biologie ou cabinet de radiologie majoritairement) **invisible au patient** mais **consultable par les professionnels habilités** ;
    - ➢ *Une liste indicative de la **typologie de documents à alimenter avec précaution** sera 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-delà de ces règles générales, une adaptation des modalités d'envoi et de visibilité devra pouvoir être réalisée au cas par cas, à l'échelle individuelle du document, sur décision médicale.*
- Des logiciels qui permettent au **professionnel qui réalise la consultation d'annonce** de **remettre en visibilité le document** « manuellement » directement dans son logiciel habituel ;
- Une « **remise en visibilité automatique » de tous les documents invisibles aux patients prévue 3 mois après l'envoi du document,** avec une information préalable du patient au **bout de 1 mois** sur l'existence

d'un document invisible dans son DMP qui nécessite une consultation d'un professionnel. Le délai de 3 mois, très supérieur aux délais habituels des annonces, a été retenu afin de maximiser les chances que les personnes bénéficient d'une information préalable sur le contenu du document, accompagnée par un professionnel de santé.

En complément des exigences du REM-HOP-DPI-Va2 sur cette thématique, des fonctionnalités ou paramétrages complémentaires peuvent être proposées par les logiciels en accord avec l'établissement tels que :

- *Une proposition au professionnel de remise en visibilité associé à la consultation d'annonce (tel qu'une proposition systématique de remise en visibilité des documents invisibles si production d'un compte-rendu "consultation d'annonce").*
- *Une liste de travail permettant le suivi du statut d'invisibilité des documents envoyés à Mon espace santé ;*
- *Le paramétrage de l'envoi à Mon espace santé au statut invisible pour certains types de documents, (par exemple certains résultats, certains services de l'établissement, certaines analyses biologiques) ;*
- *Le paramétrage de délais de remise en visibilité automatisé définis par le professionnel / établissement émetteur, pour remise en visibilité (avant les 3 mois du mécanisme automatisé de Mon espace santé).*

3.2.4 Gestion de la MSSanté

Objectifs pour le DPI en Vague 2 :

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

- Automatiser au maximum l'intégration des documents de santé reçus en établissement par MSSanté via la fonction PFI, lors que les identités nationales de santé se correspondent.
- Permettre de gérer les remplacements et suppression des documents reçus par MSSanté.

Fonctionnalités couvertes par les exigences vague 2 :

	Gestion de la MSSanté - Fonctionnalités du périmètre Vague 2	Exigences associées
3.1	**Envoi sécurisé vers la messagerie de Mon espace santé d'un patient**	
	- Fermeture du canal de communication avec le patient après envoi du message	SC.MSS/CONF.24
3.2	**Intégration de l'annuaire santé (sentinelle)**	
	- Recherche multicritère l'adresse MSSanté d'un correspondant en interrogeant l'annuaire MSSanté depuis le DPI	SC.MSS/UX.10
3.4	**Intégration et gestion des documents reçus par MSSanté**	
	- Impact de la demande de mise à jour ou suppression d'un document CDA reçu par MSS dans le logiciel avec visibilité du précédent document. - Envoi aux destinataires de la MSSanté via la fonction PFI de la mise à jour ou suppression d'un document CDA généré par le système - Informer l'utilisateur et les correspondants des documents nouveaux ou mis à jour reçus par MSSanté - Importation manuelle des documents CDA contenus dans l'enveloppe IHE.XDM et exploitation des métadonnées du document CDA afin	SC.MSS/UX.05 SC.MSS/UX.05.BIS SC.MSS/UX.38 SC.MSS/UX.39
3.5	**Intégration automatique d'un document reçu par MSSanté grâce à l'INS qualifiée**	
	- Intégration automatique des documents dont l'INS qualifiée correspond exactement - Information aux utilisateurs de la présence de nouveaux documents intégrés au systèmes et issus d'un courriel MSS	SC.MSS/UX.07 SC.MSS/UX.40
3.6	**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).	SC.MSS/UX.37

Cas d'usage et explication de l'intégration des documents dans le DPI

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

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

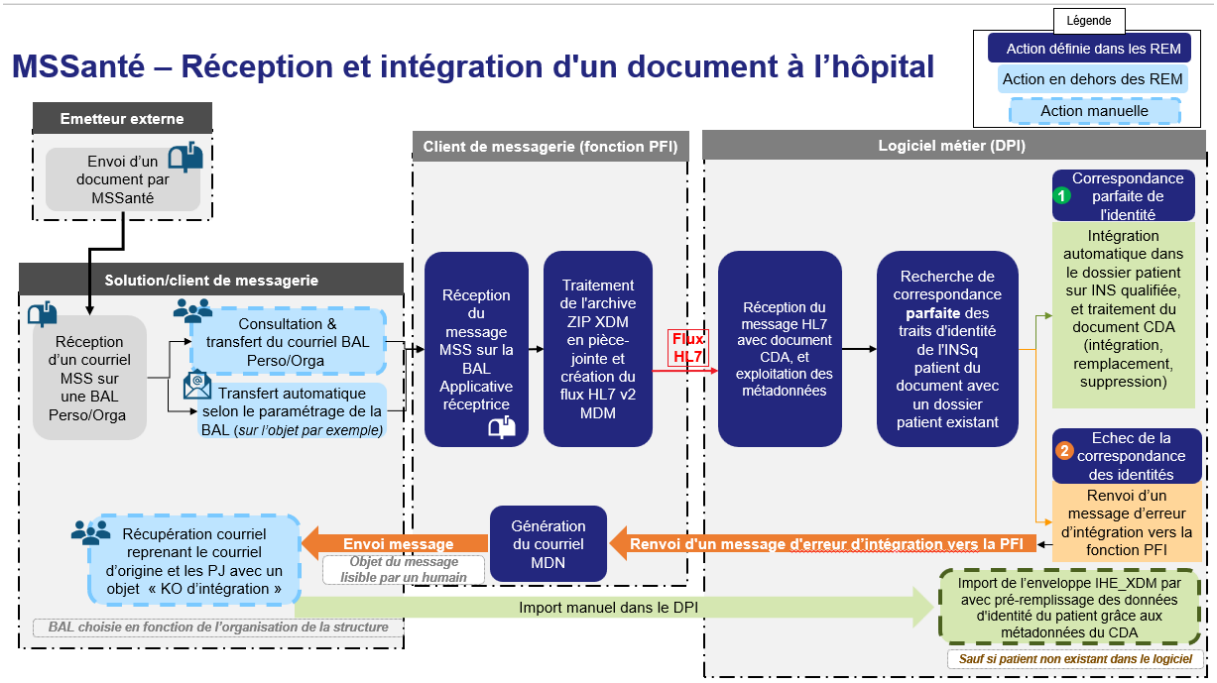
- **Echange et intégration automatique de documents lorsqu'ils sont envoyés à une BAL personnelle ou organisationnelle**. Les courriels sont consultés par un professionnel via un client de messagerie, intégré ou non au système destinataire. Cela correspond par exemple au deuxième cas d'usage du catalogue précité (Transfert d'un patient d'un CH vers un autre CH), également décrit dans le volet *Transmission de documents CDA en HL7v2*. La vague 2 propose une méthode pour intégrer automatiquement les pièces jointes dans le DPI. Comme BAL personnelles et organisationnelles ne sont pas connectés au DPI de l'établissement, le scénario d'intégration prévoit que les courriels MSSanté qui contiennent des pièces jointes IHE_XDM soit transférés manuellement ou automatiquement vers des BAL applicatives associées à des services cliniques (par exemple), sur correspondance de l'ensemble des traits d'identités des INS qualifiées.
- **Echange et intégration automatique de documents entre un système source (par exemple un SGL) et un système destinataire (par exemple un DPI).** Les échanges se font via des BAL applicatives et sont réalisés sans intervention spécifique des professionnels de santé. Ces échanges sont équivalents aux échanges de données via des messages HL7 ORU et MDM, mais le vecteur de communication est un courriel. Cela correspond au cas d'usage « Envoi/réception d'un CR de biologie médicale » du catalogue, qui est décrit dans son ensemble dans le volet *Transmission de document(s) CDA en HL7v2*.

Ainsi, la demande de traitement sur le document, incluse dans le courriel MSSanté reçue via la BAL Applicative, est transformée par la fonction PFI en un message HL7 v2 MDM (flux d'interopérabilité standardisé), transmis au DPI qui réceptionne ce message HL7. Le logiciel DPI compare l'ensemble des traits d'identités (nom de naissance, liste des prénoms, date de naissance, sexe, code INSEE du lieu de naissance, matricule INS et OID) du document reçu avec la base patients :

- **Si l'ensemble des traits d'identité correspondent parfaitement,** le logiciel métier destinataire réalise automatiquement la demande de traitement sur le document dans le dossier patient correspondant. S'il s'agit d'une mise à jour ou d'une suppression de documents, le logiciel métier destinataire viendra mettre à jour ou supprimer un document existant mais notifiera le service / professionnel et permettra de revoir l'ancienne version ou la version supprimée.
- **Si les traits d'identité ne correspondent pas,** alors le logiciel métier destinataire renvoie un message d'erreur d'intégration à la fonction PFI qui envoie un courriel à la BAL personnelle ou organisationnelle à l'origine du transfert ou à une autre BAL choisie au sein de l'établissement, pour traitement manuel de la demande. Le volet *Transmission au LPS d'un document CDA provenant d'un courriel MSSanté* spécifie le contenu d'un courriel MDN (Message Delivery Notification) que doit pouvoir générer la fonction PFI de l'établissement de soins vers la BAL personnelle ou organisationnelle à l'origine du transfert, ou à une autre BAL choisie au sein de l'établissement. Cela permet à utilisateur de consulter la BAL pour importer manuellement l'enveloppe IHE_XDM dans le logiciel. Le DPI doit alors exploiter les métadonnées pour pré-remplir la recherche patient (recherche habituelle du DPI) pour sélection manuelle du patient et rangement dans le dossier.

Il est important de préciser que le guide d'implémentation INS précise que l'exigence [EXI 11] du Référentiel INS prévoit la vérification de la cohérence de l'INS avec les traits d'identité à la réception de données de santé, sauf s'ils ont déjà été récupérés ou vérifiés par le téléservice INS chez le récepteur des données de santé. **Cette vérification est utile que si le récepteur ne dispose pas de l'INS du patient avec le statut « Identité récupérée » ou « Identité qualifiée ».**

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



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

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

Par paramétrage du client de messagerie utilisé par les utilisateurs, il est possible d'automatiser que certains documents soient transférés sur une BAL App choisie. Un exemple de règle serait : si un courriel arrive dans une BAL (ORGA) et qu'il contient une pièce jointe IHE_XDM.ZIP ou un objet formaté (XDM/1.0/DDM+<libellé> <NOM> <prénom> <date de naissance>), ce courriel peut être transféré automatiquement vers une autre BAL (par exemple, la BAL APP du service correspondant à la BAL ORG). L'émetteur du courrier transféré peut être le destinataire du courrier original, c'est-à-dire l'adresse de la BAL organisationnelle.

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

3.2.5 Identification électronique & ProSanté Connect

Objectifs pour le DPI en vague 2 :

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

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

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

Fonctionnalités couvertes par les exigences vague 2 :

	Identification électronique & ProSanté Connect - Fonctionnalités du périmètre Vague 2	Exigences associées
4.1	**Authentification et connexion sécurisée aux services socles par ProSanté Connect**	
	- Identification de l'utilisateur sur le Système avec ProSanté 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 ProSanté Connect pour la connexion au service socle sans réidentification. - Configuration de l'intégration de Pro Santé Connect en tant que client lourd en utilisant CIBA	SC.PSC.01 SC.PSC.02 SC.PSC.08 SC.PSC.13 (profil CIBA)
4.2	**Authentification sur une base de comptes locale via OIDC**	
	- Possibilité de choisir entre au moins deux fournisseurs d'identités compatibles OIDC dont l'un doit être Pro Santé Connect.	SC.SSI/IAM.80

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

Identification électronique CIBA (profil optionnel) :

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

La spécification CIBA étend OpenID Connect pour définir un flux découplé. Cela permet de décorréler l'appareil d'utilisation d'une application (e.g. ordinateur) et l'appareil utilisé pour s'authentifier (e.g. smartphone).

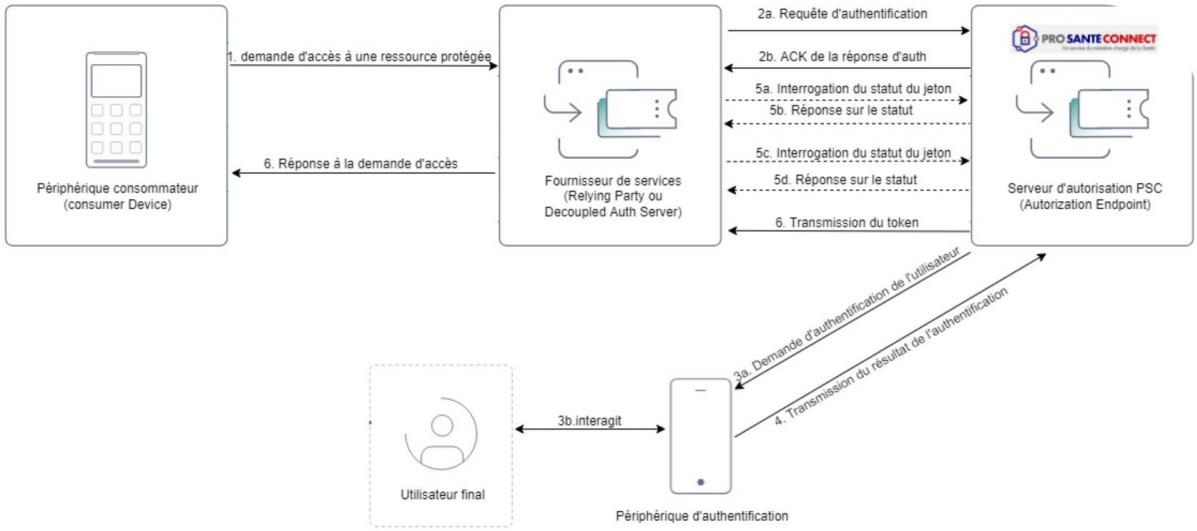


Schéma simplifié du déroulement d'une authentification CIBA

CIBA permet la mise en œuvre de nombreux cas d'usages dans un flux normalisé, et bénéficie de l'assise de la norme OpenIdConnect, déjà largement adoptée. En particulier, CIBA aide à se conformer aux cadres juridiques en définissant un protocole qui peut être utilisé pour mettre en œuvre une approche découplée pour l'authentification forte du client, comme décrit dans PSD2.

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

Rappels réglementaires sur l'identification électronique

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

3.2.6 Sécurité des SI

Objectifs pour le DPI en vague 2 :

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

- Le **Socle Commun** englobant des exigences techniques et organisationnelles visant à garantir le respect des règles de base de la sécurité des systèmes d'information ;
    - Une gouvernance efficace pour sécuriser de manière proactive les solutions, assurer la conformité réglementaire et gérer efficacement les risques de la SSI ;
    - Un renforcement de la sécurité du développement logiciel, notamment par l'application de bonnes pratiques cyber tant pour la conception de nouveaux produits que pour l'intégration de nouvelles fonctionnalités ;

  - Un maintien en conditions de sécurité des solutions grâce à un processus d'identification des vulnérabilités qui comprend des tests d'intrusion, une veille sur les menaces émergentes et une gestion proactive des correctifs de sécurité ;
  - La mise en œuvre de mesures correctives et préventives pour remédier aux vulnérabilités critiques les plus fréquentes qui pourraient être exploitées par des attaquants.
- Des **exigences IE (identification électronique)** qui visent à prendre en compte la réglementation décrite dans le référentiel d'identification électronique qui est applicable lorsque le logiciel utilise une interface utilisateur, pour renforcer la sécurité des connexions aux solutions fournissant des services numériques qui traitent des données de santé et pour une amélioration de la gestion des comptes grâce à des exigences de sécurité régissant la gestion des identités et des droits d'accès ;
- Des **exigences IAM** (Identity and Access Management) spécifiques aux solutions hospitalières et conçues pour répondre au besoin d'intégration simplifiée aux systèmes des solutions de SSO (Single Sign-On) et d'IAM.

De plus, la réalisation **d'un test d'intrusion** qui a pour but d'évaluer la sécurité de la solution candidate est un élément central du renforcement de la sécurité dans la vague 2 du Ségur numérique.

Fonctionnalités couvertes par les exigences vague 2 :

	SECURITE DES SI - Fonctionnalités périmètre Vague 2	Exigences associées
5.1	**Démarche SSI chez l'éditeur de la solution logicielle**	
	Identification des responsables de la sécurité et formalisation de leurs rôles et responsabilités. Sensibilisation des équipes aux enjeux et aux risques liés à la sécurité des systèmes d'information. Formalisation d'exigences de sécurité applicables aux tiers au travers l'élaboration d'un plan d'assurance sécurité (PAS). Mise à disposition d'un standard ou guide de bonnes pratiques visant à garantir la sécurité des développements, à la fois lors de la conception du produit ou de l'ajout de nouvelles fonctionnalités Réalisation d'une veille technologique continue autour des menaces émergentes.	*SC.SSI/GEN.01* *SC.SSI/GEN.02* *SC.SSI/GEN.03* *SC.SSI/GEN.11* *SC.SSI/GEN.20*
5.2	**Test d'intrusion**	
	Réalisation d'un test d'intrusion par solution logicielle	*SC.SSI/GEN.18*
5.3	**Gestion des comptes, des permissions et des sessions des administrateurs et des utilisateurs**	
	Séparation des droits d'accès dans le système. Limitation des comptes génériques dans des cas spécifiques.	*SC.SSI/GEN.18*
	Synchronisation régulière des données de la base de comptes avec le fournisseur d'identité ou le référentiel local (annuaire AD/LDAP de l'établissement de santé). Renforcement de la sécurité des comptes à privilèges par l'application d'une politique de mot de passe incluant différents critères tels que la longueur minimale, les délais d'expiration, le blocage des comptes, etc. Possibilité d'extraire les données de comptes afin de permettre la revue et mise à jour de ces éléments par l'administrateur	*SC.SSI/IAM.83* *SC.SSI/IAM.92* *SC.SSI/IAM.94*
	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.31* *SC.SSI/IE.32* *SC.SSI/IE.33*
	Renforcement de la sécurité des comptes, notamment lors de la connexion et de la déconnexion des systèmes.	*SC.SSI/IE.36* *SC.SSI/IE.38* *SC.SSI/IE.39*
5.4	**Gestion des sauvegardes**	
	Elaboration et l'application d'un processus de sauvegarde et de restauration.	*SC.SSI/GEN.21*
	Production et conservation de traces	
	Traçabilité des opérations effectuées au cours du cycle de vie des comptes, telles que la modification des attributs d'identité, la modification des autorisations, les tentatives de connexion, les tentatives de modification des mots de passe, etc.	*SC.SSI/IAM.91*
5.5	**Protection des informations / cryptographie**	
	Conformité des mécanismes cryptographiques utilisés et des tailles de clés correspondantes par rapport aux règles énoncées par le RGC et guides de l'ANSSI.	*SC.SSI/GEN.18*
5.6	**Réduction de la surface d'attaque du système**	
	Démarche de « durcissement » du système (réduction à l'indispensable les objets faisant partie du système, et élimination des utilisateurs et des droits non indispensables, tout en conservant les fonctionnalités requises)	*SC.SSI/GEN.18*

Précisions concernant la réalisation du test d'intrusion (exigence SSI/GEN.18)

Le test d'intrusion exigé dans le cadre du référencement vague 2 doit être réalisé, à la charge de l'Editeur, par un Prestataire d'Audit Qualifié de la Sécurité des Système d'Information (PASSI). **Attention : la réalisation d'un audit PASSI n'est pas requise**.

Le test d'intrusion se base sur :

- Le formulaire de test d'intrusion,
- Le guide d'utilisation associé.

Ces deux documents sont accessibles sur le site de l'ANS.

Le contenu du test d'intrusion se base sur le référentiel du Top 10 de l'***Open Web Application Security Project – OWASP*** (Open Web Application Security Project), qui liste les 10 risques de sécurité les plus critiques pour les applications web.

Pour chacun de ces risques, le formulaire de test d'intrusion définit les points de contrôle permettant d'évaluer le niveau d'exposition de l'application aux vulnérabilités les plus souvent exploitées par les attaquants. Ce formulaire comprend :

- Des points de contrôle communs à toutes les applications,
- Des points de contrôle spécifiques par type d'applications.

Pour chaque point de contrôle, un niveau de gravité est défini :

- Niveau de gravité haute,
- Niveau de gravité moyenne.

La Solution logicielle est conforme à l'exigence SC.SSI/GEN.18 à condition qu'elle respecte les 2 seuils de conformité aux points de contrôles suivants :

- Pour les points de contrôle de gravité haute : **0 point de contrôle KO**
- Pour les points de contrôle de gravité moyenne : **jusqu'à 10 points de contrôle KO**

Les modalités pratiques de déroulement du test d'intrusion sont indiquées dans le Guide d'utilisation disponible sur le site de l'ANS.

3.2.7 Production d'indicateurs

Objectifs pour le DPI en vague 2 :

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

Ces statistiques, se déclinent par FINESS géographique, par type de documents, par période temporelle, et concernent :

- L'alimentation des documents au DMP (via la fonction PFI) ;
- La consultation et l'intégration des documents du DMP ;
- L'envoi des documents par MSSanté (professionnelle et citoyenne de Mon espace santé) (via la fonction PFI) ;

- L'intégration des documents intégrés depuis la MSSanté (via la fonction PFI) ;
- L'information et le consentement / opposition du patient à l'utilisation de son DMP.

Fonctionnalités couvertes par les exigences vague 2 :

Autres fonctionnalités - Fonctionnalités du périmètre Vague 2	Exigences associées
Production d'indicateurs	
Fourniture de statistiques	SC.STAT/ES.01

Précisions concernant la production de statistiques

Le système DOIT fournir les statistiques suivantes :

- par FINESS géographique
- par type de documents (pour tous les documents issus du REM "liste des documents Ségur " : lettre de liaison de sortie, compte-rendu opératoire, prescription (toutes), CR ou fiche de consultation ou de visite)
- par période temporelle (à minima tous les mois de l'année courante et de l'année précédente)

Pour l'alimentation du DMP :

- Nombre de [type de document] transmis au DMP (en flux) – **réussi**
- Nombre de [type de document] transmis au DMP (en flux) – **en échec**
- Nombre de [type de document] "historique" transmis au DMP (dont la date est antérieure, avec une profondeur de 5 ans) – **réussi**
- Taux de séjours d'hospitalisation clôturés pour lequel le [type de document] a été versé au DMP

Pour la consultation du DMP :

- Nombre d'utilisateurs pour lequel une transaction de consultation DMP a été effectuée, et le ratio sur le nombre total d'utilisateurs par profil (métier)
- Nombre de documents intégrés / téléchargés (TD.3.2) provenant du DMP dans le DPI
- Taux de séjours d'hospitalisation clôturés pour lequel un utilisateur a intégré du DMP un [type de document issu de la matrice d'habilitation DMP]
- Taux de consultations pour lequel un utilisateur a intégré du DMP un [type de document issu de la matrice d'habilitation DMP]

Pour l'envoi vers la MSSanté professionnelle

- Nombre de documents envoyés aux correspondants de santé externes par MSSanté – **réussi**
- Nombre de documents envoyés aux correspondants de santé externes par MSSanté – **en échec**
- Nombre de documents avec une INS qualifiée envoyés aux correspondants de santé externes par MSSanté – **réussi**
- Nombre de documents avec une INS qualifiée envoyés aux correspondants de santé externes par MSSanté – **en échec**
- Taux de séjours d'hospitalisation clôturés pour lequel un [type de document] a été envoyé par MSSanté
- Taux de correspondants de santé ayant un mail MSSanté à qui a été envoyé un [type de document] par MSSanté

Pour l'envoi vers la MSS citoyenne de Mon espace santé

- Nombre de documents transmis au patient par MSSanté – **réussi**
- Nombre de documents transmis au patient par MSSanté – **en échec**
- Taux de séjours clôturés pour lequel un [type de document] a été envoyé par MSS au patient

- Taux de patients pour lequel un [type de document] lui a été envoyé par MSS

Pour l'intégration des documents reçus par MSSanté :

- Nombre de documents CDA intégrés automatiquement sur demande de la PFI - **réussi**
- Nombre de documents CDA intégrés automatiquement sur demande de la PFI - **en échec**
- Nombre de documents CDA intégrés manuellement par un utilisateur dans le DPI - **réussi**
- Nombre de documents non-CDA intégrés manuellement par un utilisateur dans le DPI

Pour l'information du patient à l'utilisation de son DMP :

- Taux de séjours d'hospitalisation clôturés (complets ou ambulatoires) pour lesquels l'information du patient sur l'utilisation de son DMP a été enregistrée, et pour lesquels le patient a exprimé son consentement
- Taux de séjours d'hospitalisation clôturés (complets ou ambulatoires) pour lesquels l'information du patient sur l'utilisation de son DMP a été enregistrée, et pour lesquels le patient s'est opposé
- Taux de consultations pour lesquels l'information du patient sur l'utilisation de son DMP a été enregistrée, et pour lesquels le patient a exprimé son consentement
- Taux de consultations pour lesquels l'information du patient sur l'utilisation de son DMP a été enregistrée, et pour lesquels le patient s'est opposé

Les modalités de restitution à l'établissement sont de la responsabilité de l'éditeur, notamment il est possible de proposer un tableau de bord dans le logiciel pour une meilleure représentation. Cependant dans le cadre de la vague 2, seuls les fichiers CSV exploitables sont exigés. Un exemple de formatage du CSV est fourni dans le package documentaire associé au dispositif SONS DPI.

NB 1
L'information et l'opposition du patient peuvent être soit renseignés directement dans le logiciel, soit reçus d'un système tiers
NB 2
Un séjour d'hospitalisation se caractérise par une date d'entrée et une date de sortie.
NB 3
Pour les indicateurs de taux d'envoi de documents (alimentation DMP, envoi par MSSanté) l'assiette (dénominateur) doit être adaptée en fonction des types de documents :

- *L'indicateur pour la lettre de liaison à la sortie d'un ES se calcule sur la base de tous les séjours d'hospitalisation.*
- *L'indicateur du compte-rendu opératoire (CRO) se calcule sur la base de tous les séjours avec une activité chirurgicale.*
- *L'indicateur sur les ordonnances de sortie / prescriptions se calcule sur la base des séjours pour lesquels au moins une ordonnance de sortie / prescriptions a été produite.*
- *L'indicateur sur les comptes-rendus de consultation se calcule sur la base des consultations pour lesquels un compte-rendu de consultation a été produit.*

3.2.8 Exigences issues de la vague 1 DPI

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

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

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

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

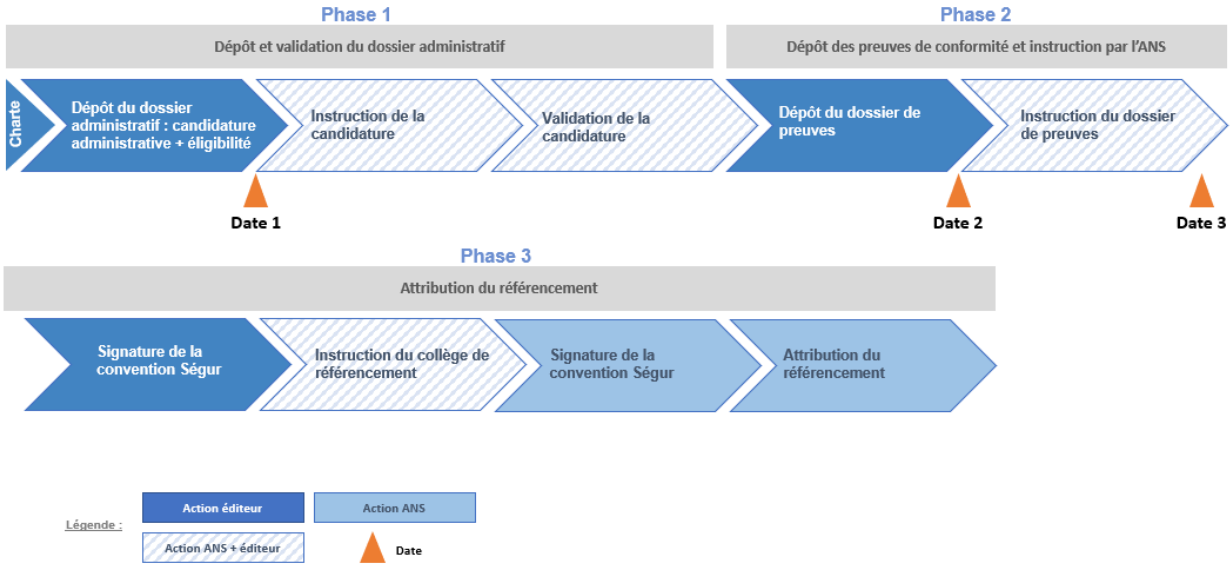
Fonctionnalités du périmètre « Vague 1 » :

CHAPITRE	FONCTIONS VA1	Exigences associées
Gestion de l'identité nationale de santé	Conformité INS et gestion du téléservice INSi	INS/va1.01 INS/va1.02 INS/va1.03 INS/va1.10 INS/va1.15 INS/va1.25 INS/va1.36 INS/va1.39 INS/va1.41 INS/va1.46 INS/va1.56 INS/va1.62 INS/va1.64
Gestion et partage des documents de santé	Production des documents au format CDA R2 conformes au CI-SIS	HOP/va1.03 HOP/va1.04 HOP/va1.06 HOP/va1.07 HOP/va1.08 DOC/va1.04 DOC/va1.05 DOC/va1.06
Consultation et alimentation du DMP / Mon espace santé	Alimentation ponctuelle de Mon espace santé Paramétrage des différentes notions de masquage et visibilité	DMP/va1.03 DMP/va1.04
Gestion de la MSSanté	Envoi de messages et de documents CDA R2 par MSSanté	MSS/va1.23 MSS/va1.24 MSS/va1.13 MSS/va1.20 HOP/va1.05
	Intégration de l'annuaire santé	ANN/va1.01 ANN/va1.02 ANN/va1.03 ANN/va1.04
Autres fonctionnalités	Portabilité des données	PORT/va1.01

4 MODALITES DE REFERENCEMENT DE LA SOLUTION LOGICIELLE

Le processus de référencement Ségur *via* la plateforme en ligne Convergence, se déroule 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



Pour accéder à la plateforme Convergence, l'Editeur doit préalablement être inscrit au fournisseur d'identité Industriels Santé Connect (iSC).

4.1 Calendrier du SONS HOP-DPI-Va2

Le système ouvert et non sélectif (SONS) pour HOP-DPI-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 HOP-DPI-Va2
19 novembre 2024 12h, ci-après **Date 1**	**REFERENCEMENT** : Date limite de dépôt du dossier administratif à l'ANS
15 décembre 2025 12h, ci-après **Date 2**	**REFERENCEMENT** : Date limite de dépôt d'un dossier complet de preuves de conformité
17 mars 2026 12h, ci-après **Date 3**	**REFERENCEMENT** : Date de fin des échanges entre l'Editeur et l'ANS pour validation du dossier de preuves de conformité
18 juin 2026 12h, ci-après **Date 4**	**FINANCEMENT** : Fin de la période de réception des demandes de financement et de versement de l'avance. Toute demande de financement et de versement d'une avance postérieure à cette date est irrecevable.
17 mars 2027 12h, 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, selon les modalités présentées à la Section 6.4.

16 juin 2027 12h, ci-après **Date 6**	**FINANCEMENT** : Fin de la période de réception des demandes de paiement du solde. 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.

4.2 Principes de Référencement

4.2.1 Solution logicielle éligible au référencement

Dans le cas où l'Editeur commercialise plusieurs Solutions logicielles couvrant le périmètre fonctionnel du DSR-HOP-DPI-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 avec un Composant principal unique ou d'une association d'un Composant principal avec un ou plusieurs Composant(s) additionnel(s) répondant aux Exigences édictées par le présent DSR. Le référencement précise le ou les Profils pour lesquels la Solution Candidate a satisfait aux Exigences.

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

4.2.2 Contrôles 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-HOP-DPI-Va2.

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

4.2.3 Audits de conformité

Les audits de conformité ont pour objet de contrôler la conformité aux Exigences du référencement de la Solution logicielle tel qu'elle est effectivement commercialisée ainsi que le caractère opérationnel de ses fonctionnalités. Ils sont réalisés majoritairement *in situ* et comprennent également les contrôles de conformité vis-à-vis des différentes obligations contractuelles.

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

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

4.2.4 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, ainsi que les informations décrivant les Solutions logicielles ayant obtenu leur référencement, en intégrant l'ensemble des informations nécessaires aux Clients pour s'assurer du respect des dispositions du SONS.

4.2 Dépôt et validation du dossier administratif

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

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

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

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

L'ANS peut solliciter l'Editeur par l'intermédiaire de la plateforme Convergence pour toute demande de complément. Si l'Editeur ne répond pas à la sollicitation dans un délai de 5 jours ouvrés à compter de celle-ci, sa demande de référencement est rejetée, 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 mentions 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 (*)
- Titre du représentant légal (*)
- Coordonnées mail et téléphoniques du représentant légal (*)
- Nom/Prénom de la personne à contacter dans le cadre du référencement (*)
- Coordonnées mail et téléphoniques de la personne à contacter (*)

Informations relatives à la Version candidate :

- Dénomination commerciale (*)
- Date prévisionnelle du dépôt de dossier de preuves complet
- Si référencé vague 1 :

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

Informations CNDA[1] :
- Numéro d'Identification Editeur (NIE délivré par le CNDA) (*)
- Numéro d'Identification Logiciel (NIL délivré par le CNDA) (*)
- Attestation de dépôt d'une demande d'obtention des labellisations CNDA (Assurance Maladie) (*)

Informations sur la Solution logicielle :
- Numéro de version technique soumise au référencement (*)
- L'Editeur transmettra à l'ANS les éléments suivants pour chaque version existante :
  - N° de version technique
  - Nom de version commerciale (plusieurs versions techniques pouvant être rattachées à un nom de version commerciale
  - L'information si la version technique est référencée en vague 1
  - Pour les Solutions logicielles pour lesquelles l'Editeur entend mobiliser des financements Ségur au titre de l'AF-HOP-DPI-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-HOP-DPI-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.

Profils pour lesquels l'Editeur demande le référencement de sa solution (*) :
- Le Profil général doit être sélectionné dans Convergence car il est obligatoire pour tous les candidats, les autres sont optionnels.
- Les Profils optionnels sélectionnés seront modifiables en fonction des temporalités suivantes :
  - Jusqu'à la **Date 2**, il est possible d'en ajouter
  - Tout au long du processus, il est possible d'en retirer

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

[1] *En conséquence, la première formalité à réaliser par l'Editeur est l'inscription auprès du CNDA afin d'obtenir ces numéros.*

4.3 Dépôt de dossier complet de preuves de conformité

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-HOP-DPI-Va2, déposées au moins une première fois par l'Editeur. Cette date ne peut être postérieure à la **Date 2**.

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

- L'ensemble des preuves attendues, en tenant compte des dispositions de la Section 3.1. Pour chaque Exigence, les preuves de conformité à fournir sont décrites dans le REM. Plusieurs preuves de conformité peuvent être demandées pour attester de la conformité de la Solution logicielle à une même Exigence (capture d'écrans, vidéos, fichiers, logs, homologations…).
    - Le dépôt des preuves peut être effectué en une fois ou par chapitre sur la plateforme Convergence.
    - Chaque preuve demandée dans Convergence est obligatoire.
- Pour chaque homologation à obtenir auprès du CNDA : l'attestation d'homologation, ou à défaut une **attestation de pré-examen** du dossier d'obtention de l'homologation concernée (ou une copie d'écran de son espace personnel CNDA) afin d'attester que l'Editeur a déposé auprès du CNDA toutes les preuves nécessaires à ladite homologation.
- Le **rapport de test d'intrusion.**
-

4.4 Instruction du dossier de preuves

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 Convergence.

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

- Le décompte du temps d'instruction des preuves de conformité par l'ANS est suspendu jusqu'à la réponse de l'Editeur.
- La place dans la file d'attente est garantie dans le cas de réponse de l'Editeur dans les 24h après notification de la demande de complément par l'ANS.
- La demande de référencement est considérée comme abandonnée en cas d'absence de réponse de l'Editeur dans les 30 jours après la sollicitation de l'ANS.

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

Les Editeurs ayant validé auprès du CNDA l'ensemble des preuves nécessaires à l'homologation (compte-rendu de pré-examen déclenchant une date d'examen) et restant dans l'attente d'une attestation d'homologation de la part du CNDA, peuvent, à titre dérogatoire de la condition définie précédemment relative à la **Date 3,** transmettre à l'ANS les éléments justificatifs au-delà de cette date limite.

Cas particulier de l'INS :

Dans le cadre de l'analyse du chapitre Gestion de l'Identité Nationale de Santé, les éditeurs non référencées vague 1 devront organiser une journée de test en visio-conférence avec l'Equipe de conformité de l'ANS.

Une fois l'ensemble des preuves du chapitre Gestion de l'Identité Nationale de Santé déposées, l'Equipe de référencement proposera sous deux semaines, une date à laquelle l'éditeur devra organiser la journée de test. L'organisation de cette journée de test incombe à l'Editeur (confirmation de la date, préparation de l'environnement ainsi que les jeux de données transmis par l'ANS, animation de la revue des scénarios de test).

L'enregistrement de la journée de test sera à la charge de l'éditeur qui devra la transmettre à l'équipe de conformité via la plateforme Convergence.

L'ANS supervise le bon déroulé des scénarios de tests et documente l'atteinte ou non des résultats.

4.5 Signature de la convention Ségur par l'Editeur et attribution du référencement

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

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

- **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 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 conformité ANS.

Utilisation du Logo de référencement Ségur

Dès lors qu'une Solution logicielle est déclarée référencée celui-ci 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

4.6.1 Création d'un compte iSC et activation de l'Espace Authentifié

Depuis la page d'accueil du Portail Industriels (https://industriels.esante.gouv.fr) en accès libre, l'Editeur peut accéder au service iSC :

- Pour s'inscrire au fournisseur d'identité iSC (en transmettant les pièces justificatives permettant de vérifier l'identité de l'entreprise de l'Editeur - Kbis, pièce d'identité du mandataire) et ainsi accéder à plusieurs fournisseurs de service,
- Pour se connecter à l'Espace Authentifié via le module d'authentification du fournisseur d'identité iSC (une fois inscrit à iSC).

Les CGU du fournisseur d'identité (iSC) sont accessibles à cette adresse : http://isconnect.esante.gouv.fr.

Une fois qu'il s'est inscrit au service iSC et qu'il a validé les CGU associées, l'Editeur peut utiliser l'Espace Authentifié.

Les CGU de l'Espace Authentifié du Portail Industriels sont accessibles à cette adresse : https://industriels.esante.gouv.fr/cgu-portail-industriels

4.6.2 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.

4.6.3 FAQ et Contact

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

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

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

4.7 Confidentialité

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

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

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

4.8 Protection des données à caractère personnel

Conformément à la réglementation européenne et française sur la protection des données personnelles, l'Editeur est informé que des données à caractère personnel sont susceptibles d'être traitées par l'ANS. Le traitement mis en œuvre a pour finalité l'instruction et le suivi du processus de référencement et de financement, le pilotage du programme de financement et du déploiement auprès des établissements et professionnels de santé des Solutions logicielles référencées par l'ANS, la gestion des sollicitations adressées par l'ANS à l'Editeur dans le cadre du pilotage du programme de référencement et de financement (par ex. des sondages ou questionnaires), le contrôle du bon usage des fonds publics versés à l'Editeur ainsi que la réalisation d'indicateurs statistiques. Des données à caractère personnel sont susceptibles d'être communiquées, dans le cadre des finalités précitées, aux partenaires de l'ANS en charge avec elle du pilotage du dispositif Ségur de financement à l'équipement (CNDA, CNAM, ministère de la santé, ASP, CNSA, CNOP, etc.). La communication de données personnelles, si elle est sollicitée par l'ANS, est nécessaire à l'instruction de la demande de référencement ou à la réalisation des autres finalités précitées. Les données collectées sont conservées pendant la durée du référencement dont bénéficie l'Editeur ainsi que pour les durées d'archivage exigées par la réglementation applicable. L'Editeur dispose d'un droit d'accès, de rectification de ses données ainsi que, dans certains cas, d'effacement, de portabilité, de limitation, et d'opposition. Les coordonnées du Délégué à la protection des données personnelles de l'ANS sont les suivantes : GIP Agence du Numérique en Santé (Délégué à la protection des données) - 2-10 Rue d'Oradour-sur-Glane 75015 Paris ou par messagerie électronique, à l'adresse suivante : dpo@esante.gouv.fr. L'Editeur dispose également du droit d'introduire éventuellement une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL).

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

4.9 Convention de preuve

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

5 GLOSSAIRE

ANS	Agence du numérique en santé, opérateur en charge de la mise en œuvre du présent dispositif.
ASP	Agence de services et de paiement, organisme en charge du traitement des demandes de financement et des paiement émises par les Fournisseurs.
CDAR2	Clinical Document Architecture, Release 2.0, standard de dématérialisation des documents médicaux électroniques exploitant la syntaxe XML (N1 : données non structurées, N3 : données structurées)
CPS	Carte de professionnel de santé permettant à son titulaire d'attester de son identité et de ses qualifications professionnelles.
CPx	Carte d'identité professionnelle électronique contenant les données d'identification de son porteur (identité, profession, spécialité) et notamment ses situations d'exercice (libéral et salarié), regroupe les carte CPE (personnel d'établissement), CDE (directeur d'établissement) et CPS (professionnels de santé)
DMP	Dossier médical partagé
ES	Etablissement de santé
FINESS	Fichier National des Établissements Sanitaires et Sociaux (FINESS), répertoire de référence pour les établissements à caractère sanitaire, social ou médico-social et de la formation aux professions sanitaires et sociales.
HAD	Hospitalisation à domicile
IHE PAM	Integrating the Healthcare Enterprise - Patient Administration Management, nom du flux dédié à la gestion des données administrative des patients
INS	Identité nationale de santé
LDAP	Lightweight Directory Access Protocol (LDAP), protocole permettant de communiquer avec différents types d'annuaires
MCO	Médecine, Chirurgie, Obstétrique
MSSanté	Messagerie sécurisée de santé
MSS-C	Messagerie sécurisée de santé citoyenne (MSS-C) permettant des échanges entre l'usager et les professionnels, Mon espace santé devient opérateur de l'espace de confiance de la MSSanté (le professionnel étant à l'initiative du premier échange)
MSS-Pro	Messagerie sécurisée de santé professionnelle (MSS pro) destinée aux professionnels de santé et qui leur permet d'échanger des données ou des documents de santé
NIE	Numéro d'Identification Editeur (NIE) : Numéro d'Identification de l'Editeur, délivré par le Centre National de Dépôt et d'Agrément (CNDA).
NIL	Numéro d'Identification Logiciel (NIL) : Numéro d'Identification Logiciel, délivré par le Centre National de Dépôt et d'Agrément (CNDA) pour l'agrément au titre du composant proposé par l'Editeur.
COFRAC	Comité français d'accréditation
PSC	Pro Santé Connect est un fédérateur de fournisseurs d'identité au standard OpenID. Pro Santé Connect permet aux professionnels de s'authentifier soit avec une e-CPS (application mobile) soit avec une carte CPS physique à tous les services numériques de santé raccordés à Pro Santé Connect.
PSY	Psychiatrie
RGS	Référentiel général de sécurité
SSR	Soin de suite et de réadaptation