MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

Délégation ministérielle au numérique en santé

Direction générale de l'offre de soins

Financé par
l'Union européenne
NextGenerationEU

Guide des prérequis

Document d'information

SÉGUR NUMÉRIQUE

Programme SUN-ES - volet 1 et 2

INSTRUCTION N° DGOS/PF5/DNS/CTO/2021/167 du 26 juillet 2021
INSTRUCTION N° DGOS/PF5/DNS/2022/40 du 9 février 2022
INSTRUCTION N° DGOS/PF5/DNS/2022/84 du 29 mars 2022

Statut : validé | *Classification : Publique* | ***Dernière mise à jour : Avril 2023***

Direction Générale de l'Offre de Soins
14, Avenue Duquesne – 75007 Paris
Mail : dgos-sun@sante.gouv.fr

Objet du document

Le présent document constitue le guide des prérequis du programme Ségur numérique usage en établissements de santé (SUN-ES) – Volet 1 et 2. Ce guide est disponible sur le site internet de la Direction Générale de l'Offre de Soins (DGOS). Il est à consulter avec les instructions N° DGOS/PF5/DNS/CTO/2021/167 du 26 juillet 2022, N°DGOS/PF5/DNS/2022/40 du 9 février 2022 et N° DGOS/PF5/DNS/2022/84 du 29 mars 2022 relatives au Programme SUN-ES.

Table des matières

Ségur de la Santé : une opportunité d'accélérer la mise en œuvre de la feuille de route nationale du numérique en santé

Une enveloppe historique de 2 milliards d'euros pour soutenir l'accélération du numérique en santé

En juillet 2020, le Ségur de la santé a été un moment clé pour le système de santé français, alors que ce dernier était confronté à une crise épidémique inédite. Il a en effet permis à ses différents acteurs – soignants, patients, administrations - de se réunir autour d'une même table, et d'identifier les principales pistes de modernisation de notre système de santé.

De cette concertation, a émergé un certain nombre de conclusions à partir desquelles les pouvoirs publics ont établi un plan d'actions structuré autour de 4 piliers :

- Pilier 1 : Transformer les métiers, et revaloriser les soignants ;
- Pilier 2 : Définir une nouvelle politique d'investissement et de financement au service de la qualité des soins ;
- Pilier 3 : Simplifier les organisations et le quotidien des équipes de santé ;
- Pilier 4 : Fédérer les acteurs de la santé dans les territoires au service des usagers.

C'est dans le cadre du pilier 2, qu'est énoncée la nécessité d'investir massivement dans le numérique pour rattraper le retard de la France dans la modernisation, l'interopérabilité, la réversibilité, la convergence et la sécurité des système d'information en santé.

Cette nécessité se traduit alors par la mise à disposition d'une enveloppe de financement historique de 2 milliards d'euros, entièrement soutenue par le Plan de Relance et Résilience Européen. Cette enveloppe se répartissant de la manière suivante :

- 1,4 milliards pour le partage de données de santé clé (sur 3 ans) ;
- 600 millions d'euros dédiés au secteur du médico-social (sur 5 ans).

Les investissements majeurs consentis doivent permettre d'accélérer la mise en œuvre de la feuille de route « accélérer le virage numérique » et bâtir in fine un parcours de santé coordonné à l'aide de services numériques ergonomiques, interopérables et faciles d'usage pour les professionnels de santé. Ces services doivent par ailleurs garantir l'accès de la personne à ses propres données de santé et préparer au mieux le déploiement en janvier 2022 de l'Espace Numérique de Santé (ENS), appelé également « Mon Espace Santé », l'outil phare du citoyen pour être acteur de sa santé.

Ainsi, les efforts à soutenir en matière de numérique, se concentrent sur les priorités suivantes :

- L'intégration des fondations numériques régaliennes, notamment l'identifiant national de santé, le cadre de sécurité et d'interopérabilité, la messagerie sécurisée et le dossier médical partagé. Cette priorité devra être soutenue auprès de toutes les parties prenantes (établissements, industriels, plateaux techniques…). Elle permettra le développement et le déploiement d'une offre logicielle de qualité.
- Le développement de cas d'usage prioritaires comme le partage de l'histoire médicale du patient, le lettre de liaison et les résultats de biologie et d'imagerie, afin de s'assurer de l'accès effectif du citoyen à ses données de santé et à leur partage entre professionnels.

Ces enjeux sont poursuivis au travers d'un programme national piloté par la Délégation ministérielle du Numérique en Santé (DNS) : **le Ségur numérique.**

Le volet numérique du Ségur : un enjeu prioritaire autour de la mise à disposition de l'espace de santé numérique citoyen « Mon espace santé »

Dès le 1er janvier 2022, l'espace numérique citoyen, appelé **Mon espace santé** proposera à l'ensemble des usagers de notre système de soin :

- **Une messagerie sécurisée** permettant des échanges d'informations et de documents (ordonnances, photos…) entre l'usager et les professionnels qui interviennent dans son parcours de soin.
- **Un agenda** permettant de consolider les différents évènements de santé : rendez-vous médicaux, hospitalisations, rappels, etc. Ces évènements pourront être alimentés par les services de prise de rendez-vous, les portails des établissements et l'usager lui-même.
- **Un catalogue de services** référencés / labellisés par la puissance publique, l'usager pourra choisir de partager les données de santé de Mon espace santé avec les applications de son choix.

La mise en place d'un tel espace implique de travailler en amont sur :

- La généralisation de l'échange et du partage fluide et sécurisé des données de santé : Il s'agit d'accélérer de façon significative la feuille de route du numérique en santé, en passant de 10 millions à 500 millions de documents médicaux échangés ou partagés d'ici 2 ans ;
- La fédération de l'ensemble des acteurs de santé intervenant dans des parcours de santé coordonnées.

Des mesures incitatives qui permettront de générer des résultats à inscrire dans la durée

Le Ségur numérique offre deux financements distincts, indépendants mais complémentaires :

- Le dispositif SONS (Système Ouvert et Non Sélectif) d'achat de l'Etat pour les comptes des acteurs de l'offre de soins : ce dispositif aide les établissements à acquérir et déployer des versions logicielles référencées Ségur, c'est-à-dire respectant l'ensemble des exigences Ségur édictées dans les Dossiers de Spécifications de Référencement (DSR). Plus précisément, il repose sur. Pour plus d'informations : https://esante.gouv.fr/segur-de-la-sante/hopital

- Le financement forfaitaire à l'atteinte de cibles d'usage SUN-ES : le financement forfaitaire à l'atteinte de cibles d'usage vise à accompagner les établissements de santé et les professionnels de santé autour de l'accélération des usages numériques : https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/segur-de-la-sante/sun-es

La dynamique obtenue grâce à ces deux leviers incitatifs doit s'inscrire dans la durée, en établissant des règles pérennes et de nature plus coercitive. Ainsi :

- Concernant le financement à l'équipement, le dispositif SONS : les exigences fixées dans les Dossiers de Spécifications de Référencement (DSR) pour les éditeurs seront rendues opposables pour chaque système d'information de santé.
- Concernant le financement forfaitaire à l'atteinte de cibles d'usage SUN-ES : les indicateurs qui déterminent ce financement auront vocation à être intégrés, après concertation, de manière pérenne au référentiel d'Incitation Financière à l'Amélioration de la Qualité (IFAQ) ainsi qu'au système de calcul déterminant le forfait structure.

Le programme SUN-ES : un programme de financement à l'usage destiné aux établissements sanitaires

Objectifs du programme

Le programme SUN-ES pour « Ségur Usage Numérique en Établissements de Santé » vise à poursuivre les efforts pour amener l'ensemble des établissements sanitaires – quels que soient leur statut, leur taille et leur activité – vers un plus grand niveau de maturité de leur système d'information, nécessaire pour assurer une meilleure prise en charge des patients grâce à l'échange et au partage sécurisé de leurs données.

Le montant alloué au financement de ce programme s'élève à 210M€ sur 3 ans (2021-2022-2023) dédiés exclusivement aux établissements sanitaires et entièrement financés par le Plan de Relance et Résilience Européen.

Le programme SUN-ES se situe dans le prolongement du programme HOP'EN et privilégie la production et la transmission de documents de santé dans le but d'enrichir, via le DMP, le nouvel espace numérique de santé « Mon espace santé » qui sera ouvert à tout citoyen français dès le début de l'année 2022. Il vise également à promouvoir l'usage des messageries sécurisés de santé dans l'espace de confiance MS Santé.

Le programme SUN-ES s'inscrit dans les grands principes du volet numérique du Ségur et particulièrement celui d'**une vision centrée sur les usages et d'une dimension inclusive pour l'ensemble des établissements sanitaires**. Il contribue ainsi à la généralisation de l'échange et du partage fluide et sécurisé des données de santé afin d'accélérer les usages, en passant de 10 millions à 500 millions de documents médicaux échangés ou partagés par an d'ici 2023.

Les usages ciblés par le programme se structurent en 2 volets :

- Le Volet 1 « alimentation du DMP » vise à soutenir le partage de documents de santé à travers l'alimentation du DMP et par extension, l'alimentation de « Mon espace santé ». Ce premier volet se décompose en 3 domaines :
  - Documents de sortie ;
  - Biologie médicale ;
  - Imagerie.

- Le Volet 2 « usage de la messagerie sécurisée de santé (MSS) » tant auprès des professionnels de santé que des patients/usagers :
  - Renforcement des usages autour de la messagerie sécurisée de santé professionnelle1 (MSS professionnelle) ;
  - Mise en œuvre de la messagerie sécurisée de santé citoyenne (MSS citoyenne) : il s'agit d'une messagerie accessible depuis « Mon espace santé » qui permettra aux professionnels de santé et établissements de correspondre avec les patients. Compte tenu du caractère nouveau de la messagerie sécurisée citoyenne, une phase d'expérimentation de la MSS citoyenne a été conduite dans 3 départements pilotes (Somme, Loire Atlantique et Haute Garonne) entre septembre et décembre 2021. Cette

[1] Pour plus d'informations sur la messagerie sécurisée professionnelle, consulter le lien suivant : https://esante.gouv.fr/securite/messageries-de-sante-mssante

phase d'expérimentation est suivie d'une phase de généralisation du déploiement de la MSS Citoyenne à l'ensemble des établissements à partir de juillet 2022.

Les usages ciblés font l'objet d'exigences qu'il est nécessaire d'atteindre si les établissements souhaitent bénéficier de soutiens financiers. Ces exigences se structurent en prérequis et en indicateurs d'usage, décrits ci-après.

Deux instructions ministérielles relatives ont été publiées respectivement au mois d'août 2021 et février 2022 afin de fixer le cadre de financement des établissements qui s'engagent dans le programme SUN-ES- **Instruction N° DGOS/PF5/DNS/CTO/2021/167 et instruction N°DGOS/PF5/DNS/2022/40 du 9 février 2022.** La Délégation du Numérique en Santé (DNS) qui pilote le Ségur numérique a confié à la Direction Générale de l'Offre de Soins (DGOS) le pilotage opérationnel du programme SUN-ES. Les Agences Régionales de Santé (ARS) sont quant à elles, chargées du suivi opérationnel de ce programme au niveau régional, en articulation avec la DGOS.

Un programme dont les exigences se structurent autour de 7 prérequis et 8 indicateurs d'usage

A l'instar du programme HOP'EN, des prérequis et des indicateurs d'usage permettent de mesurer l'atteinte du niveau de maturité attendue par les pouvoirs publics en matière d'échange et de partage de données de santé.

L'atteinte des prérequis est valide durant toute la durée du programme SUN-ES (sauf pour le prérequis PS2.2 Cybersécurité). L'établissement prouve l'atteinte des prérequis pour son premier dossier de candidature uniquement.

Présentation des prérequis sur le volet 1 et 2

- 7 prérequis ont été définis : 6 sur le volet 1 (DMP) et 1 sur le volet 2 (MSS)

  Sur le volet 1 :

  - **2 sur l'identitovigilance :**
    - Cellule d'identitovigilance opérationnelle (reprise à l'identique du P1.2 HOPEN)
    - Appropriation du référentiel national d'identitovigilance (RNIV 1 et RNIV 2) ➔ nouveau pré requis par rapport à HOP'EN
  - **2 sur la sécurité :**
    - Présence d'une politique de sécurité et d'un plan d'action SSI réalisé ainsi que l'existence d'un responsable sécurité (reprise à l'identique du P2.4 HOP'EN)
    - Cybersécurité avec la réalisation d'un audit externe de cybersurveillance au sein de l'établissement (extension du P2.5 HOP'EN)
  - **2 sur l'échange et le partage d'informations médicales :**
    - La capacité du SIH à alimenter le DMP (reprise à l'identique du P4.1 HOP'EN)
    - L'existence d'une messagerie opérationnelle intégrée à l'espace de confiance MS Santé (reprise à l'identique du P4.3 HOP'EN).

Seuls les établissements qui auront justifié de l'atteinte des 6 prérequis précédents verront leurs candidatures au volet 1 du programme SUN-ES validées par les ARS.

Sur le volet 2 :

- **1 sur l'échange et le partage d'informations médicales :**
  - La capacité technique de l'établissement de santé d'envoyer et de recevoir un message test vers/depuis la MSS citoyenne.

Seuls les établissements qui auront justifié de l'atteinte des 7 prérequis précédents (6 prérequis du volet 1 et 1 prérequis du volet 2) verront leurs candidatures au volet 2 du programme SUN-ES validées par les ARS.

Le processus de candidature est décrit dans le document « présentation détaillée du programme SUN-ES » téléchargeable depuis le lien suivant : https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/segur-de-la-sante/sun-es

Présentation des indicateurs d'usage du volet 1 et 2

Sur le volet 1 :

Le volet 1 – Alimentation du DMP – compte 6 indicateurs :

DS1.1 : Alimentation du DMP en lettre de liaison (LDL)	Taux de séjours pour lesquels le DMP a été alimenté d'une lettre de liaison de sortie au format CDA R2 niveau 1 et comprenant une INS qualifiée.
DS1.2 : Alimentation du DMP en ordonnance de sortie	Taux de séjours pour lesquels le DMP a été alimenté d'au moins une ordonnance de sortie au format CDA R2 niveau 1 et comprenant une INS qualifiée.
DS1.3 : Alimentation du DMP en compte-rendu opératoire (CRO) - BONUS	Taux de séjours pour lesquels le DMP a été alimenté d'un compte-rendu opératoire au format CDA R2 niveau 1 et comprenant une INS qualifiée.
DS1.4 : Alimentation du DMP en documents historiques du DPI BONUS	Parmi les patients déjà venus, taux de séjours pour lesquels au moins un document datant d'un ancien séjour a fait l'objet d'une alimentation au DMP, avec une INS qualifiée.
DS2.1: Alimentation du DMP en CR de biologie médicale	Taux de CR d'examens de biologie médicale structurés au format CDA R2 niveau 3 transmis au DMP avec une INS qualifiée.
DS3.1 : Alimentation du DMP en CR d'imagerie	Taux de CR d'examens d'imagerie structurés au format CDA R2 niveau 1 transmis au DMP avec une INS qualifiée.

Sur le volet 2 :

Le volet 2 – Usage de la Messagerie Sécurisée de Santé – compte 3 indicateurs :

DS 4.1 : Envoi de documents de santé aux correspondants de santé via la messagerie sécurisée de santé professionnelle	Taux de correspondants équipés d'une messagerie sécurisée de santé professionnelle auxquels des documents de santé référencés avec une INS qualifiée et structurés au format CDA ont été transmis
DS 4.2 : Envoi de messages aux patients via la messagerie sécurisée de santé citoyenne	Taux de séjours pour lesquels un message (avec ou sans pièces jointe) a été envoyé au patient par la MSS citoyenne

DS 4.3 : Présentation de la messagerie sécurisée citoyenne en Commission Médicale d'Etablissement (CME) ou équivalent	Présentation par l'établissement des fonctionnalités de la messagerie sécurisée de santé citoyenne en CME (ou instance équivalente dans les GHT et les établissements privés) ainsi que les cas d'usage pressentis

Description de la méthode de construction des prérequis

Une démarche de co-construction impliquant l'ensemble des parties prenantes de l'écosystème hospitalier

En s'appuyant sur le retour d'expérience du programme HOP'EN et au regard des enjeux du Ségur numérique, les prérequis ont été définis au cours d'ateliers de co-construction avec les acteurs de l'écosystème hospitalier sur les périodes suivantes :

- Le 13 avril et le 29 juin 2021 pour le volet 1 ;
- Le 19 octobre et le 10 décembre 2021 pour le volet 2.

Les acteurs qui ont participé à ces ateliers sont listés ci-dessous :

- **FHF** : Alexandre Mokede (Représentant FHF - SI) ; Enguerrand Habran (Représentant FHF - SI) ; Cécile Chevance (Représentante FHF) ; Kathia Barro (Représentante FHF) ; Valérie Altuzarra (DSI CHU de Bordeaux), David Cuzin (DSI GHT Atlantique 17)
- **FEHAP** : Laurent Pierre (Représentant FEHAP) ; Christophe Nicolai (Groupe hospitalier Paris Saint-Joseph) ; Laurent Uttscheid (Aider Santé) ; Jean-Pierre Grangier (Calydial) ; Gregory Chevalier (Anider)
- **UNICANCER** : Emmanuel Reyrat (Représentant UNICANCER) ; Thierry Durand (Centre Léon Berard)
- **FHP** : Bertrand Sommier (Représentant FHP) ; Christian Prudhomme (Clinique Saint Didier) ; Olivier Boixière (Vivalto) ; Pierre-André Thubet (Elsan), Dider Baty (Saint Gatien)
- **FNEHAD :** Anastasia Strizyk (Représentant FNEHAD) ; Karine Alouis (Représentante FNEHAD), Vincent Hubert (HAD France) ; Guillaume Coquet (Santelys) ; Olivier Salze (HAD Aven à l'Etel)
- **ASINHPA** : Mostafa Lassik ; Charlotte Hammel ; Jérôme Manzanares ; Elise Guittard
- **Numeum :** Mariane Cimino ; Lucile Lecomte ; Erick Vert ; Franck Toufaili ; Guillaume Lescar
- **Les ARS :** Bertrand Lerhun (ARS Bourgogne Franche Comté), Dominique Pierre (ARS Centre Val de Loire), Laurent Simon (ARS PACA), Benoit Normand (ARS Hauts de France), Bernard Geffroy (ARS Pays de la Loire), Marie Christine Labes (ARS Occitanie)
- **ANS** : Nolwenn François ; Jean-Christophe Turbatte ; Anne Lorin ; Anne Benayoune ;
- **DNS** : Jean-Baptiste Lapeyrie ; Clara Morlière
- **DGOS :** Caroline Le Gloan ; Michel Raux ; Inès Ghouil

Les participants ont également eu la possibilité de faire leurs retours et suggestions hors séance sur cette même période.

Principes et caractéristiques des prérequis

Plusieurs lignes directrices ont guidé la définition des prérequis volet 1 et 2 retenus dans le cadre du programme SUN-ES :

- **Un nombre de prérequis restreint** concentrés sur l'alimentation des outils socle que sont le DMP et la MSS ;
- Des indicateurs **simples** afin d'en faciliter l'appropriation par les établissements, les éditeurs et les ARS avant le dépôt d'une candidature ;
- **En cohérence avec les prérequis HOP'EN** et leurs seuils d'éligibilité pour accompagner progressivement la montée en maturité des infrastructures indispensables à l'échange et au partage de données de santé dans un cadre sécurisé.

Selon les bonnes pratiques qui s'appliquent à des prérequis dans une démarche qualité, les prérequis définis sont :

- **Universels**, c'est-à-dire communs à tous les établissements (quels que soient leur taille, statut et type d'activité),
- **Mesurables**,
- **Produits par les systèmes d'information des établissements** ou leur documentation associée,
- **Vérifiables** au niveau national,
- **Jugés atteignables,**
- **Conformes** aux référentiels existants (par exemple : référentiel d'interopérabilité) et aux règles de l'art.

A chaque prérequis est associé une cible d'atteinte décrite dans les fiches descriptives des prérequis (cf. document plus bas).

Structure des fiches descriptives des prérequis

De même que dans le programme HOP'EN, les prérequis du programme SUN-ES sont décrits dans des fiches regroupées par domaine. Une introduction décrit le domaine concerné ainsi que les objectifs des prérequis retenus. Les fiches descriptives des prérequis sont établies sur le modèle suivant :

- Libelle du prérequis ;
- Définition de l'indicateur ;
- Production de l'indicateur ;
- Restitution de l'indicateur.

Prérequis	**Libellé du prérequis**
Indicateur	**Libellé de l'indicateur**

Définition de l'indicateur	
Définition	Définition de l'indicateur
Déclinaison GHT	Déclinaison de l'indicateur au périmètre GHT
Valeur cible	Valeur en-deçà de laquelle un établissement de santé ou GHT ne satisfait pas aux exigences de l'indicateur
Evolution HOP'EN/Ségur	Progression entre l'indicateur du programme HOP'EN et celui présent dans le programme SUN-ES (nouvel indicateur, augmentation du seuil d'éligibilité, etc.).

Textes de référence / Liens utiles	

Production de l'indicateur	
Unité	Unité de mesure utilisée pour restituer la valeur de l'indicateur
Modalité de calcul	Formule de calcul, point méthodologique sur la construction et les modalités de recueil des valeurs d'indicateur
Période	Période de référence pour le calcul de l'indicateur
Fréquence	Fréquence minimale à laquelle doit être mesuré et transmis

Restitution de l'indicateur	
Remontée de l'information	Outil sur lequel les documents justificatifs doivent être déposés
Documents justificatifs	Liste des documents à fournir par l'établissement pour justifier de l'atteinte des prérequis
Audit	Exemples de modalités de vérification et de justification des informations *ex-post* pouvant faire l'objet d'un contrôle (liste non exhaustive)

Liste des 7 prérequis du programme SUN-ES

6 prérequis pour le volet 1

PS1 / Identitovigilance		Seuil d'éligibilité	Evolution Ségur / HOP'EN
PS1.1	Cellule d'identitovigilance opérationnelle	Fonctionnement régulier des CIV établissements/GHT (réunion *a minima* une fois par semestre) et existence de procédures de fonctionnement des CIV établissement/GHT	Reprise du prérequis P1.2 HOPEN
PS1.2	Appropriation du référentiel national d'identitovigilance (RNIV 1 et RNIV2)	Renseignement exhaustif du questionnaire d'appropriation du RNIV dans démarches simplifiées	Nouvel indicateur

PS2 / Sécurité		Seuil d'éligibilité	Evolution Ségur / HOP'EN
PS2.1	Présence d'une politique de sécurité et plan d'action SSI réalisé, existence d'un responsable sécurité.	- Existence d'une **politique de sécurité**, d'une **analyse des risques détaillée**, d'un **plan d'action associé en lien avec le plan d'action SSI de l'instruction 309 du 14 octobre 2016**, et **d'une fonction de responsable sécurité des SI (RSSI)** - Existence de la procédure de remontée des incidents de sécurité (Art. L.1111- 8-2 CSP). - Positionnement du RSSI **à privilégier** en dehors de la DSI, par exemple rattaché à la cellule qualité. - Existence d'au moins 2 rendez-vous annuels RSSI/Direction de l'établissement avec à l'ordre du jour a minima : le suivi du plan d'actions SSI et le suivi de la remontée des incidents de sécurité	Reprise du prérequis P2.4 HOPEN
PS2.2	Cybersécurité : réalisation d'un audit externe de cybersurveillance	Fourniture d'une attestation de réalisation de l'audit de cybersurveillance **par le prestataire** et signée par le directeur d'établissement	Extension du prérequis P2.5 HOPEN
PS3 / Echange et partage		Seuil d'éligibilité	Evolution Ségur / HOP'EN
PS3.1	Capacité du SIH à alimenter le DMP	DMP compatibilité (alimentation)	Reprise du prérequis P4.1 HOPEN
PS3.2	Existence d'une messagerie opérationnelle intégrée à l'espace de confiance MS Santé	Existence d'une messagerie opérationnelle raccordée à l'espace de confiance MS Santé	Reprise du prérequis P4.3 HOPEN

1 prérequis spécifique au volet 2

PS4 / Echange et partage		Seuil d'éligibilité	Evolution Ségur / HOP'EN
PS4.1	Capacité technique de l'établissement d'envoyer et de recevoir un message test vers/depuis la MSS citoyenne	L'établissement envoie au moins un message test contenant une pièce jointe vers une adresse test de la messagerie sécurisée citoyenne, conformément au référentiel #2 Clients de messageries sécurisées de santé v0.1. L'envoi des messages tests se fait à une adresse gérée par la CNAM reponse.automatique-test@patient.mssante.fr Cette adresse envoie un message de retour automatique. L'établissement possède au moins une boite de messagerie organisationnelle fonctionnelle lui permettant de recevoir et de consulter les messages envoyés par les patients.	Nouveau prérequis Ségur, non présent dans HOP'EN

Fiches descriptives des prérequis volet 1 et volet 2

PS1 : Identitovigilance

Description du domaine

Le processus d'identification du patient via l'INS est un des éléments socles pour le déploiement des politiques nationales de santé et notamment de la feuille de route du numérique en santé. Il repose sur des bases nationales de référence et comprend différentes informations permettant une identification plus fiable de chaque patient.

Pour garantir une bonne appropriation de l'INS par tous les professionnels de santé, le ministère met à leur disposition un référentiel national d'identitovigilance (RNIV). Celui-ci rassemblera in fine les règles et recommandations à respecter au sein de chaque établissement de santé pour toutes les étapes d'identification du patient dans son parcours de soins : la recherche d'antériorité, la création d'une identité numérique, la modification d'identité.

Les prérequis sur l'identitovigilance s'inscrivent en complémentarité du prérequis HOP'EN « Identification et mouvements » en venant renforcer les attendus en matière de processus de fiabilisation de l'identification des patients

Ainsi, dans le cadre du programme SUN-ES, les attentes se concentrent sur :

- Le fonctionnement de la cellule d'identitovigilance ;
- L'appropriation du Référentiel national d'identitovigilance (RNIV) : conçu par des experts du Réseau des référents régionaux en identitovigilance (3RIV) sous l'égide du Ministère des solidarités et de la santé, le RNIV a pour objet de préciser les règles et recommandations de bonne pratique à respecter par tous les acteurs de santé pour la création ou la modification d'une identité numérique (identification primaire) et pour attribuer cette identité au bon usager à toutes les étapes de sa prise en charge (identification secondaire). Le RNIV fixe le niveau minimal de sécurité que toutes les parties prenantes (usagers, professionnels de santé, agents chargés d'assurer la création et la modification des identités dans le système d'information, éditeurs informatiques, responsables de traitement de l'ensemble des applications e-santé, etc…) doivent appliquer.

Objectifs des indicateurs

Ces indicateurs ont pour objectifs de mesurer le niveau de maturité des établissements en matière d'identitovigilance.

Indicateur PS1.1 : Cellule d'identitovigilance opérationnelle

Domaine	**Identitovigilance**
Indicateur	**Cellule d'identitovigilance opérationnelle**

Définition de l'indicateur	
Définition	Une cellule d'identitovigilance est un organe ou une instance en charge de la surveillance et de la prévention des erreurs et risques liés à l'identification des patients. Elle a pour objectif de permettre de fiabiliser l'identification du patient à toutes les étapes de sa prise en charge. Son rôle est de veiller à la formation des personnels d'accueil administratif et des professionnels de santé de l'établissement/GHT en matière de surveillance et de prévention des erreurs d'identification du patient. La cellule promeut ou propose les éléments concourant à la mise en œuvre de procédures de vérification de l'identité du patient. Elle peut s'appuyer sur des mesures d'évaluation de la fiabilité de l'identification du patient à toutes les étapes de la prise en charge (indicateurs et audit) en vue d'améliorer le dispositif. La cellule doit être en capacité de fournir la documentation de la politique d'identification et de rapprochement d'identités ainsi que les procédures de création et de fusion d'identité. Une cellule d'identitovigilance opérationnelle se réunit *a minima* une fois par semestre et livre un rapport d'activité périodique comprenant : • (a) la liste des réunions effectuées de la cellule, avec une réunion par semestre *a minima* ; • (b) les incidents sur les identités relevées ; • (c) le nombre de corrections et d'améliorations auxquelles la cellule a contribué (fusion et dédoublonnage, conformément au référentiel INS).
Déclinaison GHT	Une cellule d'identitovigilance est également mise en place au niveau du GHT et s'appuie sur des CIV établissement. L'établissement support s'assure que ce prérequis est atteint pour chaque établissement candidat.
Seuil d'éligibilité	Fonctionnement régulier des CIV établissements/GHT (réunion a minima une fois par semestre) et existence de procédures de fonctionnement des CIV établissement/GHT
Evolution HOP'EN/Ségur	Reprise du prérequis P1.2 HOPEN
Textes de référence / Liens utiles	• Boîte à outils HOP'EN - Fiche méthode : Mise en œuvre de l'identito-vigilance • Guide HAS, Identification du patient à toutes les étapes de sa prise en charge, septembre 2014 • Fiche 2.3.2 « Opérer le rapprochement et la fusion des identités patients en amont de tout rapprochement fonctionnel » du guide méthodologique « Stratégie, optimisation et gestion commune d'un système d'information convergent d'un GHT »

- https://solidarites-sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance

Production de l'indicateur	
Unité	N/A
Modalité de calcul	Déclaratif
Période	Instant t (date de transmission)
Fréquence	Semestrielle

Restitution de l'indicateur	
Remontée de l'information	Saisie dans l'outil oSIS de l'indicateur
Documents justificatifs	▪ Comptes-rendus de réunions de CIV établissement/GHT qui attestent de la temporalité des réunions qui doit être a minima d'une réunion de CIV par semestre ▪ Procédures de fonctionnement de la cellule à fournir et y retrouver a minima : les procédures d'identification et de rapprochement d'identités, les procédures de création et de fusion d'identité ▪ Rapport d'activité des cellules établissement et GHT.
Audit	▪ Comptes-rendus de réunion des cellules établissement et GHT ▪ Documentation de la politique d'identification et de rapprochement d'identités ainsi que les procédures de création et de fusion d'identité ▪ Rapports d'activité périodique des cellules établissements et GHT dont le contenu est défini plus haut dans le thème « Définition de l'indicateur »

Indicateur PS1.2 : Appropriation du référentiel national d'identitovigilance (RNIV)

Domaine	**Identitovigilance**
Indicateur	**Appropriation du référentiel national d'identitovigilance (RNIV 1 et RNIV2)**

Définition de l'indicateur	
Définition	Le référentiel national d'identitovigilance (RNIV) fixe les exigences et les recommandations à respecter en termes d'identification des usagers pris en charge sur le plan sanitaire ou médico-social par les différents professionnels impliqués (structures de ville, établissements de santé, secteur médico-social, acteurs sociaux) afin de maîtriser les risques dans ce domaine. Le RNIV se substitue aux documents établissant des règles d'identitovigilance régionales. Il fixe le niveau minimal de sécurité que toutes les parties prenantes doivent appliquer pour l'identification des usagers. Les exigences et recommandations peuvent toutefois être complétées ou précisées par des documents pratiques ou des consignes particulières relevant des instances nationales, régionales, territoriales et/ou locales.

	La connaissance et l'approbation du RNIV est une condition *sine qua non* de la politique d'identification des patients.
Déclinaison GHT	L'appropriation du RNIV se fait par structure. L'établissement support s'assure que cet indicateur est atteint par chaque établissement candidat partie au GHT.
Seuil d'éligibilité	Renseignement exhaustif du questionnaire d'appropriation du RNIV (questionnaire qui devra être saisi directement dans la continuité du formulaire de candidature, dans l'outil « Démarches simplifiées »).
Evolution HOP'EN/Ségur	Introduction d'un nouveau prérequis
Textes de référence / Liens utiles	• Référentiel national d'identitovigilance

Production de l'indicateur	
Unité	N/A
Modalité de calcul	L'établissement a renseigné de manière exhaustive le questionnaire d'appropriation du RNIV
Période	Instant t (date de transmission de l'information)
Fréquence	Semestrielle

Restitution de l'indicateur	
Remontée de l'information	Remplissage du questionnaire depuis l'outil « démarches-simplifiées »
Documents justificatifs	Le remplissage exhaustif du questionnaire d'appropriation du RNIV depuis le formulaire de candidature dans démarches simplifiées
Audit	Archive des réponses de l'établissement

PS2 : Sécurité

Description du domaine

Ce domaine relatif à la sécurité des systèmes d'information vise à garantir la protection du système d'information et de ses données. Il s'agit d'installer une démarche de gestion du risque numérique, d'autant plus nécessaire dans un contexte où les cyberattaques se sont développées à l'encontre des hôpitaux ces dernières années.

La démarche de gestion et de réduction des risques est une démarche collective qui nécessite le soutien de la direction et qui doit s'exprimer dans le cadre d'une véritable politique de sécurité de l'établissement/GHT, élaborée par un responsable sécurité du système d'information, dûment mandaté.

Dans ce travail, l'établissement/GHT trouve ses orientations au sein des référentiels nationaux élaborés par l'ANS, et dans le plan d'action sur la sécurité des systèmes d'information (plan d'action SSI).

Ce plan d'action SSI a été introduit par l'instruction N°SG/DSSIS/2016/309 du 14 octobre 2016. Il vise à opérer une mise à niveau minimale de la sécurité des systèmes d'information dans toutes les structures concernées, au sein desquelles la défaillance des outils numériques représente un haut niveau de criticité. Il propose un calendrier à 6, 12 et 18 mois de réalisation de mesures prioritaires en termes d'efficacité vis-à-vis du risque de piratage informatique, etc.

Objectifs des indicateurs

Ces indicateurs ont pour objectifs de garantir :

- la mise en œuvre d'une démarche de gestion de risque organisée et soutenue par la direction de l'établissement/GHT ;
- la mise en œuvre du plan d'action SSI.

Indicateur PS2.1 : Politique de sécurité et plan d'action SSI

Domaine	**Sécurité**
Indicateur	**Présence d'une politique de sécurité et plan d'action SSI réalisé, existence d'un responsable sécurité**

Définition de l'indicateur	
Définition	Une politique de sécurité des systèmes d'information consiste en un ensemble d'exigences en matière de prévention du risque numérique et de mesures portant sur l'organisation (définition des responsabilités, formalisation et diffusion des procédures, etc.) autant que sur les caractéristiques techniques des infrastructures numériques. Elle doit être accompagnée d'actions de sensibilisation et d'amélioration au sein de l'établissement. Elle comprend une procédure de remontée des incidents de sécurité (selon l'art. L. 1111-8-2 du CSP). Cette politique de sécurité doit être mise à jour *a minima* tous les trois ans et doit être en conformité avec les différents référentiels du secteur.

	L'analyse de risque permet aux organisations de réaliser une appréciation et un traitement des risques. L'analyse de risques consiste en la combinaison de trois éléments principaux : ▪ Une identification et évaluation des ressources informatiques de l'établissement, classées par criticité ; ▪ Une analyse des menaces et qualification des risques (virus, intrusions, erreurs, incidents, etc.) auxquelles ces ressources peuvent être exposées ; ▪ L'élaboration d'un plan de traitement des risques à même de réduire la probabilité et l'impact de ces risques. Un plan d'action SSI Le plan d'action SSI, dont il est demandé la réalisation, est celui précisé par l'instruction N°SG/DSSIS/2016/309 du 14 octobre 2016 et dont l'application permet déjà de réduire significativement le risque numérique en établissement de santé. Le responsable sécurité (RSSI) est le point de contact désigné au sein de l'établissement sur le thème de la sécurité des systèmes d'information. Il doit être clairement identifié au sein de l'organisation L'exigence concerne l'existence d'une fonction de référent sécurité au sein de l'établissement, fonction qui n'est pas exercée nécessairement à temps plein. Par ailleurs, le RSSI peut être mutualisé au niveau de plusieurs structures. Le positionnement du RSSI est **à privilégier** en dehors de la DSI, par exemple rattaché à la cellule qualité.
Déclinaison GHT	Une politique de sécurité cadre des SI du GHT (PSSI GHT) existe avec une déclinaison par établissement partie. Le plan d'action sécurité du SI est réalisé au niveau de chaque établissement candidat. Un **responsable de la sécurité des systèmes d'information (RSSI) est désigné au niveau du GHT et des référents sécurité SI sont désignés au niveau de chaque établissement partie.** Le responsable de la sécurité des SI au niveau du GHT s'assure que le prérequis est atteint par chaque établissement partie au GHT candidat.
Seuil d'éligibilité	▪ Existence d'une politique de sécurité des SI ▪ Existence d'une analyse détaillée des risques, comprenant à minima : o Une identification et évaluation des ressources informatiques de l'établissement, classées par criticité ; o Une analyse des menaces et qualification des risques (virus, intrusions, erreurs, incidents, etc.) auxquelles ces ressources peuvent être exposées ➔ les risques identifiés ne doivent pas se limiter aux risques de cyberattaques o L'élaboration d'un plan de traitement des risques à même de réduire la probabilité et l'impact de ces risques. ▪ Existence d'un plan d'action associé à l'analyse de risque et en lien avec l'instruction 309 du 14 octobre 2016 ▪ Existence de la procédure de remontée des incidents de sécurité (Art. L.1111- 8-2 CSP)

	▪ Existence d'un RSSI dont le positionnement est à privilégier **en dehors de la DSI**, par exemple rattaché à la cellule qualité. ▪ Existence d'au moins 2 rendez-vous annuels RSSI/Direction de l'établissement avec à l'ordre du jour a minima : le suivi du plan d'actions SSI et le suivi de la remontée des incidents de sécurité
Evolution HOP'EN/Ségur	Reprise du prérequis P2.4 HOPEN
Textes de référence / Liens utiles	• Article L. 1110-4-1 du Code de Santé Publique • Instruction N°SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») • Mémento de cybersécurité • Fiche 2.3.7 « Mettre en place une politique de sécurité du SI » du guide méthodologique « Stratégie, optimisation et gestion commune d'un système d'information convergent d'un GHT » • Fiche 4 « Modèle de fiche de poste de RSSI de GHT » du guide méthodologique « Stratégie, optimisation et gestion commune d'un système d'information convergent d'un GHT » • Foire aux questions sur la stratégie, l'optimisation et la gestion commune d'un système d'information convergent • Boîte à outils HOP'EN - Fiche méthode : Politique de sécurité et plan d'action SSI • Boîte à outils HOP'EN - Fiche méthode : Rôles de RSSI et DPO

Production de l'indicateur	
Unité	N/A
Modalité de calcul	Déclaratif
Période	Instant t (date de transmission des informations)
Fréquence	Semestrielle
Restitution de l'indicateur	
Remontée de l'information	Saisie dans l'outil oSIS de l'indicateur.
Documents justificatifs	▪ Politique de sécurité des SI formalisée, signée par le directeur d'établissement, à jour depuis moins de 3 ans ▪ Analyse détaillée des risques, comprenant a minima : o Une identification et évaluation des ressources informatiques de l'établissement, classées par criticité ; o Une analyse des menaces et qualification des risques (virus, intrusions, erreurs, incidents, coupures électriques, etc.) auxquelles ces ressources peuvent être exposées ; o L'élaboration d'un plan de traitement des risques à même de réduire la probabilité et l'impact de ces risques. ▪ Plan d'action associé à l'analyse de risque et en lien avec l'instruction 309 du 14 octobre 2016 ▪ Procédure de remontée des incidents de sécurité (Art. L.1111- 8-2 CSP)

	▪ Document attestant de l'existence de la fonction de RSSI à travers la désignation claire d'un RSSI ▪ Calendrier ou compte-rendu des réunions RSSI/Direction attestant d'au moins 2 rencontres annuelles et ceci sur la période des deux dernières années : Si le justificatif est le calendrier, préciser l'ordre du jour des points traités lors de ces points de sorte à vérifier que les 2 points suivants a minima ont été traités : le suivi du plan d'actions SSI et le suivi de la remontée des incidents de sécurité
Audit	▪ Revue des documents justificatifs ▪ Revue du plan d'action SSI et planning de mise en œuvre pour les actions concernées

Indicateur PS2.2 : Audit externe de cybersurveillance

Domaine	**Sécurité**
Indicateur	**Réalisation d'un audit externe de cybersurveillance**

Définition de l'indicateur	
Définition	Un audit de sécurité est l'un des moyens à disposition de tout organisme pour éprouver et s'assurer du niveau de sécurité de son système d'information. En pratique, il permet de mettre en évidence les forces, mais surtout les faiblesses et vulnérabilités du système d'information. Ses conclusions permettent d'identifier des axes d'amélioration, de proposer des recommandations et de contribuer ainsi à l'élévation de son niveau de sécurité, en vue, notamment, de son homologation de sécurité. Il est demandé à l'établissement de faire réaliser un audit de cybersurveillance dont les caractéristiques minimales sont définies par le service national de cybersurveillance en santé prévu dans l'action 9 de la feuille de route « accélérer le virage numérique » et décrit dans la doctrine technique du numérique en santé. Il s'agit d'un audit des domaines des structures de santé exposés sur Internet ainsi que des accès VPN afin de détecter d'éventuelles vulnérabilités. Cet audit ne constitue pas un outil d'évaluation exhaustif de la sécurité d'un SI et ne permet pas au **responsable de traitement** de se soustraire à une **analyse de sécurité de l'ensemble de ses actifs numériques**. Cet audit recouvre les prestations suivantes, il: • cartographie et détermine la surface d'attaque d'un système d'information à partir d'Internet ; • détecte les vulnérabilités qui affectent le système d'information d'une organisation ; • détecte une éventuelle fuite de données (code-sources, identifiants, données à caractère personnel, etc.) visant le système d'information.

	Le rapport de cyber-surveillance fourni doit présenter :
	• le périmètre de l'évaluation avec la liste des domaines et sous-domaines, avec une cartographie des systèmes détectés ;
	• une synthèse managériale permettant de prendre rapidement connaissance du niveau de sécurité constaté et de la typologie des vulnérabilités ;
	• une synthèse technique présentant :
	  ○ les vulnérabilités détectées par niveau de criticité,
	  ○ un plan d'actions de remédiation hiérarchisé ;
	• le détail des vulnérabilités identifiées avec pour chacune :
	  ○ la criticité,
	  ○ le type de vulnérabilité (ou catégorie, telle que usurpation d'identité, défaut de configuration, …),
	  ○ le SI affecté,
	  ○ la description de la vulnérabilité,
	  ○ la recommandation associée en vue de sa correction.
	
	Dans le cas d'un audit global qui concernerait plusieurs établissements d'un GHT/groupe, si un seul rapport d'audit est produit (rapport global versus rapport individuel), celui-ci doit citer explicitement les structures couvertes par l'audit et comprendre les résultats de l'audit pour chacun des établissements concernés si des spécificités sont relevées ainsi qu'une proposition de plan d'actions par établissement
	
	Cet audit devra être réalisé par une entreprise spécialisée dans le domaine de la sécurité des SI. Compte-tenu du caractère sensible du résultat de ces audits pour les établissements, il est fortement recommandé de porter une **attention particulière au choix de la société prestataire et d'éviter de recourir à une société soumise à des lois extra-européennes** ayant pour objectif la collecte de données ou métadonnées des commanditaires sans leur consentement préalable.
	
	Les audits ADS, mais aussi SILENE, réalisés par l'ANSSI ne peuvent pas être recevables comme élément de preuve pour les prérequis « audit de cybersurveillance » pour les programmes HOP'EN et SUN-ES, car leurs périmètres sont différents (même s'il y a une partie de recouvrement avec SILENE).

Déclinaison GHT	Applicable par établissement. L'établissement support s'assure que ce prérequis est atteint par chaque établissement partie au GHT.
Seuil d'éligibilité	Fourniture d'une attestation de réalisation de l'audit de cybersurveillance signée par le directeur d'établissement : • Cette attestation de réalisation doit être produite par le prestataire et signée par le directeur d'établissement. • Cette attestation doit préciser que l'audit de cybersurveillance couvre le périmètre des domaines exposés sur Internet et des accès VPN.

	Pour la fenêtre 1 du volet 1 du programme, il est possible pour les établissements de présenter un bon de commande d'un audit de cybersurveillance, en lieu et place de la réalisation effective de celui-ci, à la condition que cet audit soit réalisé avant la fin de la période d'instruction des dossiers par les ARS, à savoir le 31 décembre 2021. **A partir de la fenêtre 2, seule l'attestation de la réalisation effective des audits est acceptée comme pièce justificative.** Pour les fenêtres 1, 2 et 3 : Seuls les audits réalisés après 2020 sont acceptés. Les audits réalisés avant 2020 ne sont pas acceptés. **Pour la fenêtre 4 : Seuls les audits réalisés après 2021 sont acceptés. Les audits réalisés avant 2021 ne sont pas acceptés.**
Evolution HOP'EN/Ségur	Ce prérequis correspond au P2.5 du programme HOP'EN avec l'évolution suivante. Le bon de commande ne permet plus désormais de valider ce prérequis. Seule la présentation d'une attestation de réalisation de l'audit valide le prérequis.
Textes de référence / Liens utiles	• L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur (https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/) • Prestataires d'audit de la sécurité des systèmes d'information référentiel d'exigences (https://www.ssi.gouv.fr/uploads/2014/12/PASSI_referentiel-exigences_v2.1.pdf) • Arrêté du 14 septembre 2018 fixant les règles de sécurité relatives à la sécurité des systèmes d'information des OSE (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037444012&dateTexte=&categorieLien=id) • Feuille de route « Accélérer le virage numérique »

Production de l'indicateur	
Unité	N/A
Modalité de calcul	Déclaratif
Période	Instant t (date de transmission des informations)
Fréquence	Semestrielle

Restitution de l'indicateur	
Remontée de l'information	Saisie dans l'outil oSIS de l'indicateur
Documents justificatifs	▪ Attestation de réalisation de l'audit de cybersurveillance fournie par le prestataire et signée par le directeur d'établissement ▪ Attestation qui doit stipuler que l'audit a bien couvert les domaines exposés sur Internet ainsi que les accès VPN ▪ **Bien prendre connaissance de l'item « Définition de l'indicateur » qui précise les conditions d'éligibilité de cet audit**.
Audit	▪ Périmètre de l'audit

	▪ Revue du rapport d'audit, et des recommandations associées le cas échéant

PS3 : Echange et partage

Description du domaine

Ce domaine vise à garantir la compatibilité des SIH avec les outils socle (DMP et MSSanté), en particulier avec la perspective du lancement de Mon espace santé (anciennement appelé espace numérique de santé) en janvier 2022.

A travers ces outils, il s'agit de développer de façon sécurisée l'échange et le partage d'information entre la ville et l'hôpital mais aussi entre les professionnels et les patients dans une optique de parcours de soins coordonné et centré sur le patient.

Les exigences formulées concernent la mise en place de :

- L'alimentation du DMP pour offrir au patient et aux professionnels de santé qui le soignent une vue globale de son dossier médical ;
- Un renforcement des usages autour de la messagerie professionnelle pour favoriser la coordination entre les professionnels de santé ;
- Le développement des usages autour d'un nouveau service d'échange : la messagerie sécurisée Mon espace santé (ou MSS citoyenne) qui permettra aux patients et aux professionnels d'échanger dans un cadre sécurisé.

Objectifs des indicateurs

- Capacité du SIH à alimenter le DMP ;
- Existence d'une messagerie sécurisée intégrée à l'espace de confiance MS Santé : messagerie sécurisée de santé professionnelle (MSS professionnelle) et citoyenne (MSS citoyenne)

Indicateur PS3.1 : Capacité du SIH à alimenter le DMP

Domaine	**Echange et partage**
Indicateur	**Capacité du SIH à alimenter le DMP**

Définition de l'indicateur	
Définition	Alimentation du DMP par un ou plusieurs applicatifs du SIH directement ou indirectement.
Déclinaison GHT	Applicable par établissement. L'établissement support s'assure que ce prérequis est atteint par chaque établissement partie au GHT.
Seuil d'éligibilité	DMP compatibilité (alimentation)
Evolution HN-HOP'EN	Reprise du prérequis 4.1 HOP'EN
Textes de référence / Liens et références utiles	▪ Instruction N°SG/DSSIS/2016/147 du 11 mai 2016 relative au cadre commun des projets d'e-santé ▪ Instruction N°SG/DSSIS/DGOS/DGCS du 13 mars 2018 relative à l'accompagnement en région de la généralisation du dossier médical partagé (DMP) ▪ Contenu du DMP : https://www.service-public.fr/particuliers/vosdroits/F10872

Production de l'indicateur	
Unité	N/A
Modalité de calcul	Remontée automatique à partir des données de la CNAM
Période	Instant T (date de transmission des informations)
Fréquence	Semestrielle

Restitution de l'indicateur	
Remontée de l'information	DMP compatibilité (remontée automatique à partir des données de la CNAM), indication du nom de la solution et de l'éditeur ou du dispositif permettant la DMP compatibilité.
Documents justificatifs	▪ Preuve d'alimentation fournie par les services de la CNAM Si les données d'alimentation du DMP ne sont pas présentes dans l'oSIS, il est possible pour l'ES de déposer les pièces justificatives suivantes : ▪ Justificatif attestant de la validation de la CME d'alimenter le DMP ▪ Précision de la version de la solution logicielle utilisée et captures d'écran de la solution logicielle démontrant l'existence des fonctions d'alimentation du DMP et le fait que ces fonctions sont bien opérationnelles.
Audit	L'audit pourra s'effectuer avec l'utilisation des données produites par la CNAM.

Indicateur PS3.2 : Capacité à émettre par messagerie sécurisée MS Santé

Domaine	**Echange et partage**
Indicateur	**Existence d'une messagerie opérationnelle intégrée à l'espace de confiance MSSanté**

Définition de l'indicateur	
Définition	Existence d'une messagerie opérationnelle intégrée à l'espace de confiance MSSanté.
Déclinaison GHT	Applicable par établissement. L'établissement support s'assure que ce prérequis est atteint par chaque établissement partie au GHT.
Seuil d'éligibilité	Existence d'une messagerie opérationnelle raccordée à l'espace de confiance MSSanté.
Evolution HN-HOP'EN	Reprise du prérequis P4.3 HOPEN
Textes de référence / Liens et références utiles	▪ Instruction N°DGOS/PF5/2014/361 du 23 décembre 2014 relative à l'usage de la messagerie sécurisée MS Santé dans les établissements de santé ▪ Site dédié à la messagerie sécurisée MS Santé ▪ « MSSanté, le kit de déploiement » mis à disposition par l'ANS ▪ Boîte à outils HOP'EN - Fiche méthode : Messagerie Sécurisée de Santé

Production de l'indicateur	
Unité	N/A
Modalité de calcul	Remontée automatique à partir des données de l'ANS
Période	Instant T (date de transmission des informations)
Fréquence	Semestrielle

Restitution de l'indicateur	
Remontée de l'information	Messagerie de santé conforme à l'espace de confiance MS Santé (remontée automatique à partir des données de l'ANS : indicateur de l'oSIS « a intégré l'espace de confiance » à « Oui » - onglet « Messagerie sécurisée de santé »), nom de la solution et de l'éditeur.
Documents justificatifs	▪ Preuve d'alimentation fournie par les services de la CNAM ▪ Si les chiffres d'activité de la MSS fournis par l'ANS ne sont pas disponibles dans l'oSIS, l'établissement a la possibilité de déposer la preuve d'envoi d'un message par messagerie sécurisée de santé (copie d'écran ou trace générée par le logiciel lors de l'envoi d'un message)
Audit	L'audit pourra s'effectuer avec l'utilisation des données de l'ANS.

Indicateur PS4.1 : Capacité technique de l'établissement d'envoyer et de recevoir un message test vers/depuis la MSS citoyenne

Domaine	**Echange et partage**
Indicateur	**Capacité technique de l'établissement d'envoyer et de recevoir un message test vers/depuis la MSS citoyenne**

Définition de l'indicateur	
Définition	Compte tenu du caractère nouveau de la messagerie sécurisée de santé citoyenne, il est indispensable de poser comme exigence le socle technique de la MSS citoyenne à partir duquel des usages pourront être générés dans de bonnes conditions. Ce prérequis vise donc à vérifier la capacité technique de l'établissement à engager un dialogue avec le patient, au travers de la MSS citoyenne
Déclinaison GHT	Applicable par établissement. L'établissement support s'assure que ce prérequis est atteint par chaque établissement partie au GHT.
Seuil d'éligibilité	L'établissement envoie au moins un message test contenant une pièce jointe vers une adresse test de la messagerie sécurisée citoyenne, conformément au référentiel #2 Clients de messageries sécurisées de santé v0.1. L'envoi des messages tests se fait à une adresse gérée par la CNAM - reponse.automatique-test@patient.mssante.fr. Cette adresse envoie un message de retour automatique. La pièce jointe demandée doit se présenter sous la forme d'une archive ZIP au format IHE_XDM contenant un ou plusieurs documents CDA avec un niveau de structuration au format CDA R2 Niveau 1 à minima. L'établissement possède au moins une boite de messagerie organisationnelle fonctionnelle lui permettant de recevoir et de consulter les messages envoyés par les patients. Le seuil d'éligibilité fait l'objet d'une adaptation uniquement la fenêtre 2 du programme. Sur la fenêtre 2, il est possible pour les établissements de présenter un bon de commande de déploiement de solution logicielle permettant l'envoi à la MS Santé avec possibilité de joindre des documents au format CDA dans les messages émis. Ce bon de commande doit stipuler que la solution sera déployée au plus tard avant la fin de la période d'instruction des dossiers par les ARS, à savoir le 30 juin 2022.
Evolution HN-HOP'EN	Nouveau prérequis Ségur, non présent dans HOP'EN
Textes de référence / Liens et références utiles	

Production de l'indicateur	
Unité	N/A
Modalité de calcul	Déclaratif par l'établissement + remontée automatique à partir des données de la CNAM
Période	Instant T (date de transmission des informations)
Fréquence	Semestrielle

Restitution de l'indicateur	
Remontée de l'information	Saisie dans l'outil oSIS
Documents justificatifs	Exclusivement sur la fenêtre 2 : il est possible pour les établissements de présenter un bon de commande de déploiement de solution logicielle permettant l'envoi à la MS Santé avec possibilité de joindre des documents au format CDA dans les messages émis. Ce bon de commande doit stipuler que la solution sera déployée au plus tard avant la fin de la période d'instruction des dossiers par les ARS, à savoir le 30 juin 2022. **Sinon :** Transmission des preuves d'envoi du message test contenant une pièce jointe : • Capture d'écran du message test dans laquelle on identifie l'adresse émettrice et l'adresse destinataire et la pièce jointe sous la forme d'une archive ZIP au format IHE_XDM et PDF ; • **OU** trace qui montre qu'un message a été envoyé avec l'information sur l'adresse émettrice, l'adresse destinataire et la présence d'une pièce jointe au format IHE XDM et PDF **ET** Transmission de la capture d'écran du message retour reçu de la part de messagerie test de la CNAM. A noter que le message test de l'établissement peut être transmis depuis une boite applicative, organisationnelle ou nominative. Quel que soit le type de boite de messagerie utilisée pour faire le test, il est demandé à l'ES de posséder au moins une boite organisationnelle et de la déclarer dans les pièces justificatives du volet 2 : • L'établissement possède au moins une boite de messagerie organisationnelle fonctionnelle lui permettant de recevoir et de consulter les messages envoyés par les patients.
Audit	L'audit pourra s'effectuer avec l'utilisation des données de la CNAM.