MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Doctrine technique du numérique en santé

I. La démarche, la synthèse, le macro-planning, la feuille de route 2021, la démarche d'opposabilité et le schéma d'architecture cible

Version : 2020 | Date : janvier 2021

FEUILLE DE ROUTE
DU NUMÉRIQUE EN SANTÉ

Doctrine technique du numérique en santé

Version 2020

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

SOMMAIRE

OBJET DU DOCUMENT

Avec la présentation de la **feuille de route « Accélérer le virage numérique »** par Agnès BUZYN - Ministre de la Santé et des Solidarités - le 25 avril 2019, **le cap en matière de numérique en santé à horizon 2024 a été fixé**.

La feuille de route « accélérer le virage numérique » :

Au travers de cinq orientations déclinées en trente actions, cette feuille de route a pour ambition de mettre le numérique au service du parcours de santé des usagers et des professionnels qui les prennent en charge.

Ce document constitue la **doctrine technique** sur laquelle s'appuiera la mise en œuvre de la feuille de route « accélérer le virage numérique ». Un **schéma d'urbanisation cible** complète cette doctrine technique.

Ce document a pour objectif de décrire le cadre technique et le cadre d'urbanisation dans lequel devront s'inscrire les services numériques d'échange et de partage de données de santé, en cible (à horizon trois ans) et en trajectoire. Il s'adresse aux porteurs des services numériques, qu'ils en assurent la maîtrise d'ouvrage (groupements régionaux d'appui au développement de la e-santé, établissements de santé…) et/ou la maîtrise d'œuvre (éditeurs de solutions, intégrateurs…) ainsi qu'aux usagers des services numériques (professionnels de santé et du médico-social ou usagers des services numériques de santé au sens large).

Le périmètre couvert :

A l'image de la feuille de route « accélérer le virage numérique », cette doctrine technique se concentre sur l'échange et du partage de données de santé, sur les champs sanitaire et médico-social.

Ce cadre national comprend également la prise en compte des enjeux et des obligations liées au **déploiement de la e-santé en Europe** et auxquels la France prend part.

Si cette doctrine aborde la mise en œuvre de la feuille de route « accélérer le virage numérique » sous l'angle de l'urbanisation, **elle reste néanmoins attachée au cadre de valeur humaniste** présenté dans #MaSanté2022. La France s'engage à porter également ce message dans ses contributions européennes et internationales en matière de développement de la e-santé.

La version 2019 de la doctrine technique du numérique en santé a été publiée en janvier 2020. Comme s'y était engagé le Ministère des Solidarités et de la Santé, la doctrine fait l'objet d'une mise à jour annuelle. Il s'agit de tenir l'écosystème de la santé numérique, informé des évolutions et avancées de chaque chantier, d'informer sur les priorités à venir et les implications techniques qu'elles sous-tendent. Ce présent document a fait l'objet d'une large concertation publique et constitue dorénavant la version 2020 de la doctrine technique du numérique en santé.

SYNTHESE

La synthèse présentée ci-après résume les principes clés de la doctrine technique du numérique en santé.

Les fondements de la doctrine technique

1. **La présente doctrine constitue l'une des actions de la feuille de route « Accélérer le virage numérique »**[1] présentée par Agnès BUZYN - Ministre de la Santé et des Solidarités - le 25 avril 2019. Elle matérialise le principe « d'Engagement collectif vers une e-Santé au service des usagers ». Elle fournit le cadre dans lequel devront s'inscrire les services numériques d'échange et de partage de données de santé dans les trois prochaines années (description de la cible et de la trajectoire). Cette doctrine est portée par la Délégation Ministérielle du Numérique en Santé. Elle remplace le Cadre Commun des Projets de e-Santé en région[2], document de référence publié en 2016. La doctrine technique du numérique en santé est mise à jour annuellement.

2. **La présente doctrine s'adresse au monde de la santé au sens large**. Elle concerne l'ensemble des acteurs du sanitaire (professionnels de la ville comme de l'hôpital), et ceux du médico-social et du social, impliqués dans les parcours de santé. Elle s'adresse aux porteurs des services numériques, qu'ils en assurent la maîtrise d'ouvrage (groupements régionaux d'appui au développement de la e-santé, établissements de santé…) et/ou la maîtrise d'œuvre (éditeurs de solutions, intégrateurs…) ainsi qu'aux usagers des services numériques (professionnels de santé et du médico-social ou usagers des services numériques de santé au sens large).

3. **La présente doctrine est applicable à l'ensemble des services numériques manipulant de la donnée de santé et utilisés sur le territoire français**, en métropole comme dans les Départements, Régions et Collectivités d'outre-mer ;

4. **A travers la présente doctrine technique, l'Etat joue son rôle de régulateur, d'architecte et d'urbaniste des services numériques en santé. Il vise à :**
   - Promouvoir la e-santé en donnant un cadre clair et partagé, notamment à travers la stabilisation et clarification de certains principes en attente d'arbitrages et de doctrine claire depuis de nombreuses années ;
   - Engager les acteurs privés et publics à développer des services utiles aux usagers et aux professionnels, dans le respect des valeurs et du cadre définis par la puissance publique ;
   - Permettre à l'ensemble des acteurs concernés d'apporter sa pierre à l'édifice.

[1] esante.gouv.fr/sites/default/files/media_entity/documents/Dossier_virage_numerique_masante2022.pdf
[2] esante.gouv.fr/sites/default/files/media_entity/documents/instruction_cadre_commun.pdf

5. **A travers la présente doctrine technique, l'Etat installe le principe d'Etat-plateforme :**
   - La doctrine technique n'a pas de valeur réglementaire, en revanche :
     - Une démarche d'opposabilité est portée par les différents chantiers identifiés dans la doctrine technique du numérique en santé.
     - Les référentiels de ces différents chantiers ont vocation à être rendus opposables tout comme les procédures d'évaluation et de certification permettant de mesurer la conformité des systèmes d'information ou des services ou outils numériques.
     - La conformité des services numériques à la doctrine fera l'objet d'un contrôle et d'une publicité nationale.
   - L'Etat met à disposition de l'écosystème de la santé numérique le cadre technique de référence reposant sur trois piliers fondateurs : l'éthique, la sécurité et l'interopérabilité.
   - Ce cadre technique de référence contient :
     - Un ensemble de documents de référence[3], de gisements de données[4] nationaux et outils[5] constituant les **référentiels socles** ; Les services numériques de santé disposent ainsi de règles et fondations communes pour identifier électroniquement les utilisateurs de ces services où qu'ils soient sur le territoire français, pour protéger les données de santé qu'ils contiennent, pour communiquer avec le même langage dans le respect des standards internationaux. Les données de santé peuvent ainsi être collectées, échangées et partagées en toute confiance, de manière fluide, sur tout le territoire français.
     - Des **services socles** : le DMP, qui répond au besoin de partager des informations et données médicales, structurées ou non structurées, utiles à la coordination des soins en tout point du territoire ; les messageries sécurisées de santé (MSSanté) pour sécuriser l'échange d'informations de santé ; la e-prescription pour simplifier, sécuriser et dématérialiser le circuit de transmission de l'ordonnance depuis la prescription jusqu'à la dispensation par le prescrit (pharmacien, infirmière, kiné,…) ; des outils pour faciliter la coordination dans les territoires (cahier de liaison, gestion d'alertes, réseau social entre professionnel, fédération d'agendas, ...). Ces outils s'inscrivent dans le programme e-Parcours.
     - Des **plateformes numériques nationales** pour permettre, dans le respect des règles d'urbanisation, d'interopérabilité, de sécurité et d'éthique, la multiplication de services à valeur ajoutée pour les usagers, regroupés dans un espace commun pour leur donner plus de visibilité et faciliter les échanges de données entre eux. Les plateformes seront constituées d'un volet destiné aux usagers l'« Espace Numérique de Santé (ENS) » et d'un volet ciblant les professionnels de santé, du médico-social et du social, le « bouquet de

[3] Documents de référence : Cadre d'urbanisation sectoriel, Cadre d'Interopérabilité des SI de santé (CI-SIS), Politique Générale de Sécurité des SI de santé (PGSSI-S)

[4] Gisements de données de référence : Identifiant national de santé (INS), Annuaire Santé (RPPS, …), Répertoire opérationnel des ressources (ROR), Serveur multi-terminologie de santé

[5] Outils de référence : France Connect et l'application carte vitale (ApCV), Pro santé connect et la e-cps

services » (BSP). Dans la logique de « store d'applications », toutes deux permettent de référencer les applications privées et publiques respectant les règles fixées par cette doctrine technique et le référentiel de labellisation qui présentera les critères à respecter. La troisième plateforme, le Health Data Hub, favorise l'analyse des données à grande échelle au bénéfice de tous.

Le cadre technique de référence permet donc à l'écosystème industriel concerné, de disposer d'un environnement numérique stabilisé et de se concentrer sur des fonctionnalités et services métier à valeur ajoutée auxquels tout usager ou professionnel aura facilement accès à travers une plateforme nationale sécurisée.

6. **La présente doctrine présente les leviers prévus par l'Etat pour réguler le numérique en santé, soutenir l'informatisation des structures de santé et favoriser l'innovation** :
   - L'Etat met à disposition un outil web en ligne appelé *Convergence* pour permettre aux promoteurs de services numériques d'évaluer la conformité de leur solution aux principes d'urbanisation, de sécurité et d'interopérabilité décrits dans cette doctrine technique. En complément de l'outil convergence, des outils d'évaluation de conformité par domaine métier (ex. télémédecine, médico-social, maison et centre de santé…) sont mis en œuvre. Après le périmètre des services régionaux et des solutions industrielles, la démarche de convergence est étendue aux structures afin qu'elles puissent également évaluer leur maturité par rapport aux actions de la feuille de route du numérique en santé. Ce dispositif est associé à un environnement de test national facilitant les tests d'interopérabilité entre les solutions. Les résultats de ces tests et évaluations seront rendus publics, des contrôles aléatoires de vérification pourront être prévus par les services de l'Etat ;
   - L'Etat soutient la modernisation des systèmes d'information des établissements de santé (programmes HOP'EN, Simphonie, convergence des systèmes d'information des GHT) et des structures médico-sociales (programme ESMS numérique), ainsi que l'innovation (réseau national de structures de santé dites « 3.0 »). En septembre 2020, l'Etat a lancé la plateforme G_NIUS[6] (ex Lab' e-Santé). Cette plateforme, Guichet National de l'Innovation et des Usages en e-Santé, oriente, informe et met en relation l'ensemble des acteurs de la santé numérique pour faciliter l'innovation collective et valoriser les réussites de terrain. Les innovateurs sont guidés pour trouver rapidement la bonne information, le bon interlocuteur. La boussole G_NIUS guide l'utilisateur dans sa recherche d'informations sur le cadre technique de référence matérialisé par la présente doctrine technique, l'Info financement permet aux éditeurs de retrouver les sources de financement françaises et européennes pour concrétiser leurs projets innovants.

[6] https://gnius.esante.gouv.fr/

7. **La présente doctrine s'enrichit des contributions de l'écosystème de la santé et est mise à jour annuellement**.
    - Elle fait l'objet de consultations publiques, ouvertes à tous. Chacune des contributions déposées sur la plateforme de concertation est analysée et la doctrine mise à jour quand cela le nécessite. La doctrine technique du numérique en santé est publiée sur le site de l'Agence du numérique en santé : esante.gouv.fr.
    - Elle s'enrichit des travaux portés par la cellule éthique et par les groupes de travail du Conseil du Numérique en Santé qui œuvrent sur les thèmes de la formation au numérique en santé, de la fracture numérique et e-santé, de l'évaluation des bénéfices de la e-santé et du développement économique en France et à l'international des entreprises françaises.

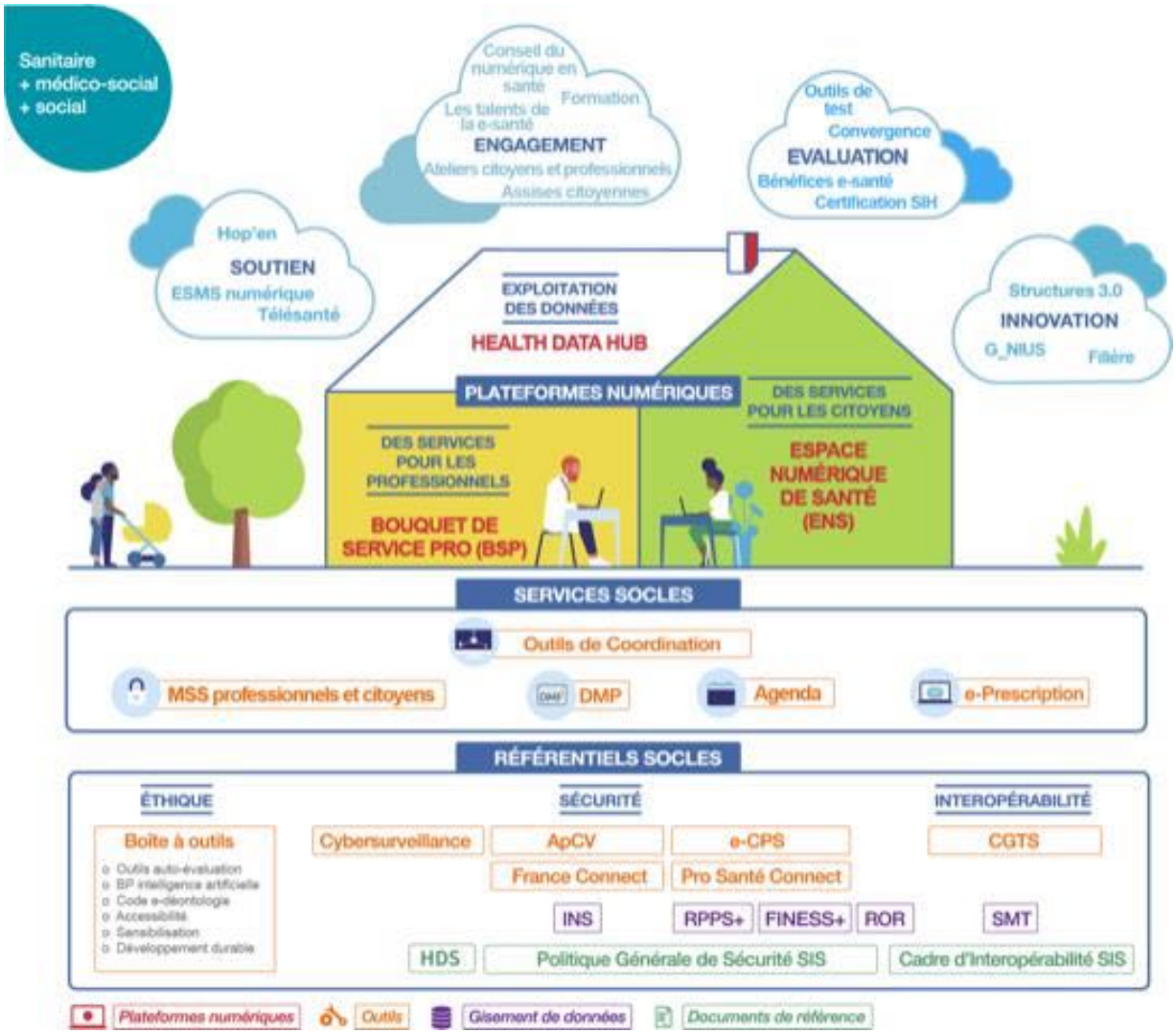
8. **La présente doctrine inclut la synchronisation avec la trajectoire de la mise en place du cadre de e-santé européen**
    - Avec l'adoption de la directive 2011/24/UE[7] relative aux droits des patients en matière de soins transfrontaliers, l'Europe s'est engagée dans une feuille de route e-santé. Le déploiement de la e-santé au niveau Européen vise à permettre la circulation des citoyens en termes de parcours de soins et de permettre la coordination des soins en Europe. Cela signifie que l'Europe a la volonté de rendre interopérables les systèmes de santé de l'UE, de développer l'accessibilité des soins transfrontaliers et souhaite encourager les coopérations européennes en matière de soins.
    - Depuis, plusieurs programmes et actions ont alimenté cette feuille de route, et la France en a été partie prenante.
    - La crise pandémique de 2020 a montré la pertinence et l'urgence de cette vision, et la nécessité de l'encourager. Les actions en cours devraient donc être accélérées par le nouveau programme EU4Health dans le cadre de l'Europe de la santé souhaitée par la Présidente de l'Union Européenne dans son discours sur l'état de l'Union (octobre 2020) : « Notre objectif est de protéger la santé de tous les citoyens européens. La pandémie du coronavirus a souligné la nécessité d'une coordination renforcée au sein de l'UE, de systèmes de santé plus résilients et d'une meilleure préparation aux crises futures. Nous n'abordons plus les menaces transfrontières pour la santé de la même manière. Aujourd'hui débute la mise en place d'une Union européenne de la santé, destinée à protéger les citoyens en les dotant de soins de qualité en cas de crise et à équiper l'Union et ses États membres pour prévenir et gérer les urgences sanitaires qui touchent l'ensemble de l'Europe. »
    - La feuille de route nationale doit non seulement intégrer ces engagements européens, mais peut également les inspirer.

[7] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:FR:PDF

Les composants du cadre de référence mis à disposition par l'Etat

9. Le cadre d'urbanisation sectoriel des systèmes d'information de santé décline les règles d'urbanisation appliquées au numérique en santé

- Le cadre d'urbanisation sectoriel des systèmes d'information (SI) de santé décline les règles d'urbanisation issues du cadre d'urbanisation européen et du cadre d'urbanisation des SI de l'Etat.



Le schéma ci-dessus permet de visualiser synthétiquement les composants du cadre de référence de la e-santé. Ils sont décrits ci-après du bas vers le haut : d'abord les référentiels socles, puis les services socles et enfin les plateformes nationales. Certains composants sont impliqués dans le cadre de référence ou les initiatives européennes en cours ou planifiées.

DANS LES REFERENTIELS SOCLES :

10. L'identifiant national de santé (INS) pour référencer et partager les données de santé.

- L'INS est le NIR (numéro d'inscription au répertoire national d'identification des personnes physiques, plus communément appelé « numéro de sécurité sociale ») lorsqu'il sert pour la facturation – à défaut le NIA (numéro identifiant attente) - associé à des traits d'identité de l'état civil. Des solutions alternatives seront proposées dans les versions ultérieures de cette doctrine pour les personnes ne disposant ni d'un NIR ni d'un NIA (numéro NNP pour les bénéficiaires de l'AME, etc.). ;
- Issu du SNGI, l'INS est diffusé par la Cnam à travers son téléservice INSi (recherche et vérification). Ce dispositif permet la récupération de données, officielles, fiabilisées et actualisées, à partir d'une source certifiée et reconnue par les autorités administratives ;
- L'utilisation de l'INS accompagnée des procédures d'identitovigilance est obligatoire à compter du 1er janvier 2021 ;
- L'INS est l'identifiant pivot obligatoire pour l'échange et le partage des données de santé et documents médicaux qui pourra remplacer ou être référencé comme champ additionnel des identifiants locaux (IPP, identifiant régional…) dont certains sont amenés à disparaitre progressivement au profit de l'INS ;
- L'Etat fournit aux acteurs de la prise en charge, un accès aux données de l'identité INS (Matricule INS complété par un OID, nom de naissance, prénom(s) de naissance, sexe, date de naissance, lieu de naissance) issues des bases de référence (répertoires RNIPP/SNGI) par la mise à disposition du téléservice (INSi). Le téléservice INSi propose deux opérations : l'une permettant de récupérer une identité INS (opération de récupération) et l'autre permettant de vérifier une identité INS (opération de vérification), accessibles pour les acteurs de santé.
- Il permet à toutes les unités de production de soins (établissements de santé, maisons de santé pluriprofessionnelle, cabinet de ville…) de référencer ses documents et données de santé avec l'identifiant national du patient ;
- Un référentiel national d'identitovigilance (RNIV) a été construit en 2020 avec le réseau des référents régionaux d'identitovigilance (3RIV) et mis à concertation. Il sera rendu opposable début 2021.
- L'éventuelle fonction de "rapprochement" (SRRI) des SRI disparait.
- L'éventuelle fonction de "GAM régionale" (SRI) / "référentiels d'identité commun aux services régionaux" des SRI peut perdurer. En effet, 2 options d'urbanisation sont possibles pour les régions : Option 1 : Chaque service régional dispose d'une base d'identité qui lui est propre ; Option 2 : Les services régionaux s'appuient sur une "GAM régionale". Dans les deux cas, il est obligatoire d'y référencer l'identité INS dans les conditions prévues par le référentiel INS, le référentiel national d'identitovigilance, le guide d'implémentation de l'INS et le guide d'intégration du téléservice INSi.

11. Les dispositifs d'identification électronique des usagers auprès des téléservices de santé sont prévus :

- Pour assurer l'identification électronique aux services de santé en ligne, des niveaux de garantie sont attendus de la part des fournisseurs d'identité, au 1er janvier 2023 dans un premier temps, il est attendu, pour ces services numériques, l'atteinte d'un niveau de garantie équivalent eIDAS « faible », mais renforcé. L'objectif, à terme, d'être de niveau de garantie « substantiel » lorsque des données de santé à caractère personnel sont traitées ;
- L'application Carte Vitale (ApCV) servira de mécanisme de référence pour l'identification électronique ;
- Une généralisation de l'utilisation de France Connect, permettra l'accès à une variété de fournisseurs d'identité et une fluidification des échanges de données entre les services.

12. Un annuaire national contenant l'identification nationale des utilisateurs de services de e-santé :

- L'Annuaire Santé géré par l'Agence du numérique en santé (ANS) contient et publie d'ores et déjà les données d'identification des professionnels de santé, référencés avec leur identifiant national RPPS ou ADELI. L'identifiant ADELI (qui concerne les infirmiers par exemple) disparaitra prochainement au profit du numéro RPPS ;
- L'Annuaire Santé permet de disposer d'une photographie exhaustive de l'identité professionnelle de l'acteur de santé (état civil, diplômes, spécialités). Les données sont certifiées ;
- L'Annuaire Santé a vocation à contenir les données d'identification de tous les professionnels qui ont besoin d'utiliser des services de e-santé (secrétaires médicales, aides-soignants, gestionnaires de cas MAIA, …). Ces derniers se voient progressivement doter d'un identifiant de portée nationale.
- L'annuaire contient également les données d'identification des structures / personnes morales (FINESS, SIRET).

13. Une identification numérique des acteurs de santé auprès des services de e-santé facilitée par le fournisseur d'identité sectoriel ProSanté Connect et la e-CPx :

- L'application e-CPS permet aux professionnels de s'identifier électroniquement auprès de services en ligne avec un smartphone ou une tablette, en conservant le même niveau de sécurité que la carte CPS ;
- Le fournisseur d'identité sectoriel santé (ProSanté Connect) réalise l'identification électronique forte à la place des services numériques de santé et décharge les éditeurs de cette gestion et des contraintes techniques associées. Il sera obligatoire au 1er janvier 2023 pour tous les services partagés, intégrant des services partagés, ou faisant l'objet de connexions externes (correspondants de ville se connectant au SI d'un établissement, accès par un portail web (hors VPN) aux applications d'un établissement, etc.) ;
- E-CPS et ProSanté Connect sont adossés à l'Annuaire Santé et proposés gratuitement par l'ANS pour accélérer le développement de la e-santé avec des mécanismes d'identification électronique forte ;
- La mise en œuvre de ProSanté Connect avec le dispositif e-CPS pour tous les professionnels intégrés dans le référentiel national est prévue pour 2021 ;
- Les conditions d'une identification électronique pour les structures sont également mises en œuvre. L'identification électronique des personnes morales s'appuie sur les données de l'annuaire santé notamment FINESS et SIREN / SIRET et sur les certificats IGC-Santé qui contiennent l'identifiant de portée nationale, vérifié à l'enrôlement.

14. La politique générale de sécurité des systèmes d'information de santé (PGSSI-S) fixe les exigences de sécurité des services numériques en santé :

- La PGSSI-S se compose de référentiels pour fixer et décrire les exigences de sécurité des systèmes d'information portant sur :
  - L'identification des acteurs de santé et médico-sociaux ;
  - L'identification des patients et usagers du système de santé ;
  - L'imputabilité (gestion de preuve et traçabilité) ;
  - La force probante des documents de santé (référentiel publié en 2020) ;
  - Le renforcement technique du niveau de sécurité.
- La PGSSI-S contient également des guides de bonnes pratiques pour accompagner les acteurs de santé, en décrivant les bonnes pratiques organisationnelles et techniques à appliquer ;
- Elle doit être compatible avec le cadre européen, et intégrer les recommandations de bonnes pratiques européennes, éventuellement internationales dans sa feuille de route dont la prise en compte des initiatives européennes en matière de cybersécurité.
- La doctrine d'identification électronique sera déclinée dans quatre chapitres de la PGSSI-S qui deviendront opposables en application de l'article L1110-4-1[1] du code de la santé publique (référentiels de sécurité et d'opposabilité) et des articles de loi créés par l'ordonnance identification électronique. Ces quatre chapitres sont :
  - IE des usagers (personnes, citoyens, patients, aidants, etc.) et leur identité INS ;
  - IE des acteurs de santé personnes physiques - ASPP (ex : médecins, secrétaires médicales, etc.) et leur identité RPPS ;
  - IE des acteurs de santé personnes physiques - ASPM (ex : centre hospitalier, CPTS, service numérique référencé dans le store de l'ENS, etc.) et leur identité FINESS/SIREN ;
  - Gestion des contrôles d'accès.
- Des travaux sont en cours pour :
  - Renforcer la gouvernance autour de la PGSSI-S ;
  - Rendre opposables les référentiels et s'assurer de leur prise en compte au niveau des services numériques en santé financés sur fonds publics ;
  - Accompagner les acteurs de santé et du médico-social.

15. L'hébergement des données de santé est encadré par une évaluation de conformité à un référentiel de certification :

- L'Etat a mis en place une procédure de certification pour l'hébergement de données de santé à caractère personnel sur support numérique (qui remplace l'ancienne procédure d'agrément). Elle concerne à la fois les fournisseurs d'infrastructure physique et les fournisseurs de service d'infogérance ;
- L'activité d'hébergement de données de santé est encadrée par l'évaluation de conformité des services d'hébergement de données de santé proposés par l'hébergeur à un référentiel de certification, réalisée par un organisme de certification accrédité par le COFRAC ;
- Ce cadre de protection des données de santé est une référence en Europe et dans le monde ;
- En 2020, l'hébergement des données de santé évolue de manière à prendre en compte les apports du Règlement Général sur la Protection des Données (RGPD), notamment sur la notion de responsabilité conjointe et les nouveaux droits des personnes.

16. Le Répertoire Opérationnel des Ressources (ROR) constitue le référentiel de données de description de l'offre de santé :

- Le Répertoire Opérationnel des Ressources (ROR) constitue le référentiel de données de description de l'offre de santé commun aux secteurs sanitaire (ville et hôpital) et médico-social ;
- Il a vocation à offrir une description exhaustive, homogène et opérationnelle de l'offre de santé sur le territoire national afin d'alimenter les applications métiers qui facilitent l'orientation et la mise en œuvre d'un parcours usager fluide. Pour ce faire, un nouveau jalon sera franchi fin 2020 avec l'initialisation du peuplement du ROR pour l'offre de ville, l'offre médicosociale et des établissements de santé étant d'ores et déjà intégrée ;
- Il a pour vocation d'être également la référence unique pour tout projet international impliquant l'offre de santé en France. Afin d'améliorer le service de consommation de l'offre de santé par l'ensemble des services numériques, l'architecture ROR va devenir nationale d'ici 2022.

17. Les référentiels d'interopérabilité se composent du cadre d'interopérabilité et des terminologies de santé et permettent ainsi d'intensifier le partage et l'échange des données de santé entre solutions :

- Le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) contient des spécifications d'interopérabilité qui pointent vers les nomenclatures à utiliser directement et les jeux de valeurs adaptés au contexte. Il s'enrichit au fil de l'eau en fonction des cas d'usage métiers remontés par les projets nationaux, territoriaux, ainsi que par les projets européens ou par les industriels, et déposés auprès du guichet unique. Il contient également depuis 2020 les données du CI-TLSi de la Cnam.
- La trajectoire de ces référentiels doit veiller à les rendre compatibles avec les référentiels européens.
- Le centre de gestion des terminologies de santé (CGTS) est un guichet national public qui distribue gratuitement les terminologies de santé et autres ressources sémantiques, et permet ainsi le codage non ambigu d'une information. Il est également l'interlocuteur des organisations internationales en charge des terminologies de santé.
- Courant 2020, ces ressources sémantiques seront rendues accessibles via un serveur multi-terminologies (SMT) dans un format réutilisable par les industriels pour l'intégration dans les logiciels de professionnels de santé, en garantissant leur qualité et leur distribution sécurisée par une licence ouverte.

DANS LES SERVICES SOCLES :

18. Le dossier médical partagé (DMP) est le service national de référence pour le stockage et le partage des documents de synthèse (dont le volet de synthèse médicale) et des données de santé du patient utiles à la coordination des soins :

- Le DMP est le seul et unique outil permettant le stockage permanent des documents médicaux de synthèse utiles au parcours de santé (synthèse médicale, compte rendu hospitalisation, compte rendu imagerie, résultats de biologie …). Les services numériques régionaux et locaux s'adossent à cette infrastructure pour partager des documents médicaux. ;
- Les actions de déploiement réalisées par l'Assurance Maladie depuis 3 ans ont permis d'atteindre en 2020 plus de 9,5 millions de DMP ouverts, la labellisation de plus de 90 logiciels de cabinet pour les Professionnels de Santé (LGC, LGO et Terminaux DMP compatibles), l'alimentation du DMP par 24 Centres Hospitaliers Universitaires, 600 établissements de santé et 1124 EPHAD ;
- Le DMP est alimenté/consulté par le professionnel via son logiciel métier « DMP compatible » (logiciel de ville ou système d'information hospitalier). Le DMP fait partie des services prévus au bouquet de services aux professionnels ;
- A partir du 1er janvier 2022, il sera consulté et alimenté par l'usager via son Espace Numérique de Santé (ENS) en version web et mobile ;
- La loi évoluera afin de caler la création automatique de l'ENS avec la création d'un DMP pour chacun (sauf opposition de l'usager ou de son représentant légal) ;
- En complément, afin de faciliter le transfert des données médicales des patients en Europe, un projet « Patient Summary » (volet de synthèse médical européen) est en cours de déploiement. L'ANS a été désignée point de contact national pour la France. Une infrastructure permettant la transmission du Patient Summary (envoi/réception) a été adossée à l'infrastructure nationale par l'ANS : il s'agit du NCPeH (National Contact Point for eHealth) qui fait donc partie d'un réseau comportant une infrastructure de ce type par pays européen. Le NCPeH permettra dès 2021 aux professionnels de santé de recevoir les patient summaries européens pour les patients étrangers suivis en France. Cette infrastructure a été auditée en 2020 par la Commission européenne.

19. L'espace de confiance MSSanté permet de sécuriser les échanges de données de santé :

- Le système de messageries sécurisées de santé (MSSanté) est un « espace de confiance » national. Il dispose d'une « liste blanche » des opérateurs (établissements de santé, éditeurs de logiciels, organismes publics, …) dont les domaines de messagerie sont autorisés à échanger des données de santé ;
- La cible à 2022 est de couvrir l'ensemble des professionnels et structures de santé, médico-sociaux et sociaux afin de favoriser la coordination dans le cadre de la prise en charge des usagers, garantissant l'identité et la légitimité de chacun de leur correspondant ; de permettre à un professionnel exerçant en établissement de santé ou en ville, d'échanger de manière sécurisée avec un usager du système de santé depuis son Espace Numérique de Santé (ENS) ; de permettre l'interopérabilité et la sécurité des différents types de messageries professionnelles de santé, incluant les messageries dites "instantanées" ;
- L'ANS met à disposition des opérateurs MSSanté et des éditeurs de logiciel les référentiels et moyens leur permettant de développer l'usage de leur service de messagerie facilitant la pratique des professionnels selon le contexte de leur exercice et de leur secteur d'activité. Au cours du T4 2020, la démarche d'opposabilité des référentiels MSSanté a été lancée. Le référentiel opérateur sera rendu opposable courant 2021.
- L'ANS débute les travaux permettant de rendre l'échange avec l'Espace de Confiance MSSanté accessible à d'autres acteurs amenés à échanger des données de santé, y compris en dehors des situations de prise en charge existantes.

- L'Espace Numérique de Santé portera la fonctionnalité de messagerie permettant aux usagers d'échanger avec un professionnel de santé dès lors que ce dernier en aura été à l'initiative. Cette messagerie sécurisée sera un opérateur de l'espace de confiance de la MSS facilitant ainsi les échanges avec les professionnels de santé. Un prototype de messagerie sécurisée de santé entre usager et professionnels est en cours depuis 2020 et se poursuivra dans le premier trimestre 2021.

20. Un service national de référence pour la production et l'utilisation de prescriptions dématérialisées :

- Le service e-Prescription proposé par la Cnam est destiné aux professionnels de santé de ville et des établissements de santé, pour les prescriptions exécutées en ville, et consiste à dématérialiser le circuit de l'ordonnance entre les médecins et les prescrits (pharmacien, infirmière, masseurs-kinésithérapeutes,). Le patient reçoit toujours une version papier de sa prescription ;
- L'ensemble des données est stocké au sein d'une base de données sécurisée de l'Assurance Maladie ;
- Le dispositif actuel e-prescription est en cours de généralisation pour les médicaments et les dispositifs médicaux. Il sera étendu à d'autres types d'actes en 2021 (biologie, infirmier, auxiliaires médicaux.
- Un projet européen est actuellement en cours de déploiement en Europe et devrait à terme intégrer la France.

21. Des outils de coordination mis à disposition dans les territoires par les Agences régionales de santé (ARS), appuyés par les Groupements régionaux d'appui au développement de l'e-santé (GRADeS) - programme e-Parcours :

- Les services numériques de coordination des parcours sont définis au niveau régional pour être construits au plus proche des usages et du terrain sur les territoires.
- Ces services sont des outils de workflow au service des professionnels de santé, médico-sociaux et sociaux dans le cadre de la coordination des parcours et de la collaboration pluriprofessionnelle au service du patient, dans une logique de prise en charge décloisonnée ;
- Ils viennent en complément des outils métier déjà existants (système d'information hospitalier, logiciel du professionnel libéral, …) et s'appuient impérativement sur les services socles (service de partage avec le DMP et d'échange avec MSSanté) et les fondations de la présente doctrine (référentiels de données de référence, outils socles documents de référence…) ;
- Un accord-cadre national (4 titulaires par lot) facilite l'acquisition de solutions homogènes par les GRADeS sur l'ensemble du territoire et respectant le cadre d'urbanisation national. Ce cadre permettra également de favoriser la mutualisation des innovations entre régions.

DANS LES PLATEFORMES NATIONALES :

22. L'Etat organise la mise en œuvre de trois plateformes pour favoriser et démultiplier la mise à disposition de nouveaux services numériques dans le respect des règles d'urbanisation, d'interopérabilité, de sécurité et d'éthique :

- L'Espace Numérique de Santé (ENS) permettra à chaque usager, bénéficiaire de l'assurance maladie au 1er janvier 2022 de choisir et d'accéder à des services numériques de santé (tels que le DMP, la messagerie sécurisée entre professionnels et usagers, l'agenda santé consolidant les différents évènements santé de l'usager, et de nombreuses autres applications proposées par les secteurs privés et publics) de manière sécurisée et fluide ;

- Les professionnels peuvent quant à eux accéder au bouquet de services (BSP) qui pourra s'enrichir, à partir du 1er janvier 2022, des services communicants avec l'ENS ;

- Ces plateformes constituent donc un réceptacle aux applications proposées par les acteurs publics et privés qui s'y inscrivent. L'objectif est simple : permettre aux usagers et professionnels de santé de trouver leurs repères dans des espaces numériques fiables et simples d'accès. Ces espaces numériques se constitueront étape par étape, avec l'évolution de services existants, grâce à des méthodes de co-conception et via des appels à projet ;

- L'ENS aura fait l'objet d'un large travail de cadrage sur toute l'année avec un début des chantiers opérationnels en fin d'année 2020 pour un premier rendez-vous en juillet 2021 avec le pilote et en janvier 2022 pour la généralisation en l'ensemble du territoire. L'année 2020 aura permis aussi pour l'ENS d'assurer l'appels à candidatures auprès de l'écosystème pour la réalisation des POC pour les différentes fonctions des plateformes, de définir le processus de référencement des applications du catalogue. Les travaux de cadrage du BSP ont quant à eux, débutés au dernier trimestre 2020.

- En rassemblant les données de santé dans un même schéma d'urbanisation sécurisé, les pouvoirs publics se donneront les moyens de les analyser à grande échelle et de les rendre accessibles au bénéfice de tous. C'est l'objectif du Health Data Hub, la plateforme des données de santé, en cours de déploiement ;
- La plateforme technologique est désormais ouverte aux premiers projets et un premier catalogue de bases de données composé des bases les plus prometteuses sera mis à disposition des chercheurs, mais aussi des associations de patients et citoyens, des institutions, des start-ups, et des différentes parties prenantes du secteur de la santé. Les services seront ouverts à tous à horizon 2021-2022.
- Le Health Data Hub est également le représentant en France du projet de construction du European Health Data Space ; cette action conjointe européenne est en cours de préparation et démarre en 2021.

Les modalités d'opposabilité des principes et de vérification du respect des règles et de la doctrine technique

23. La loi prévoit l'opposabilité des référentiels de sécurité et d'interopérabilité :

- Les référentiels, tout comme les procédures d'évaluation et de certification permettant de mesurer la conformité des systèmes d'information ou des services ou outils numériques, présentés dans la doctrine technique sont opposables par arrêtés et s'imposent à l'ensemble des acteurs de l'écosystème ;
- La démarche d'opposabilité est portée par les différents chantiers identifiés dans la doctrine technique du numérique en santé. Elle a vocation à faire partie des différents outils permettant de maitriser collectivement la trajectoire globale de mise en œuvre de la feuille de route, en s'appuyant sur trois piliers : une vision partagée des étapes et objectifs, la concertation et une démarche progressive, sur plusieurs axes au niveau de chaque référentiel ;
- La trajectoire de cette démarche s'appuie sur deux axes majeurs : rendre opposables en déclinaison de l'article L 1110-4-1 les référentiels des briques et cas d'usage du SEGUR et rendre opposables en déclinaison de l'article L 1110-4-2 les procédures d'évaluation et de certification et publier les solutions conformes à ces référentiels ;

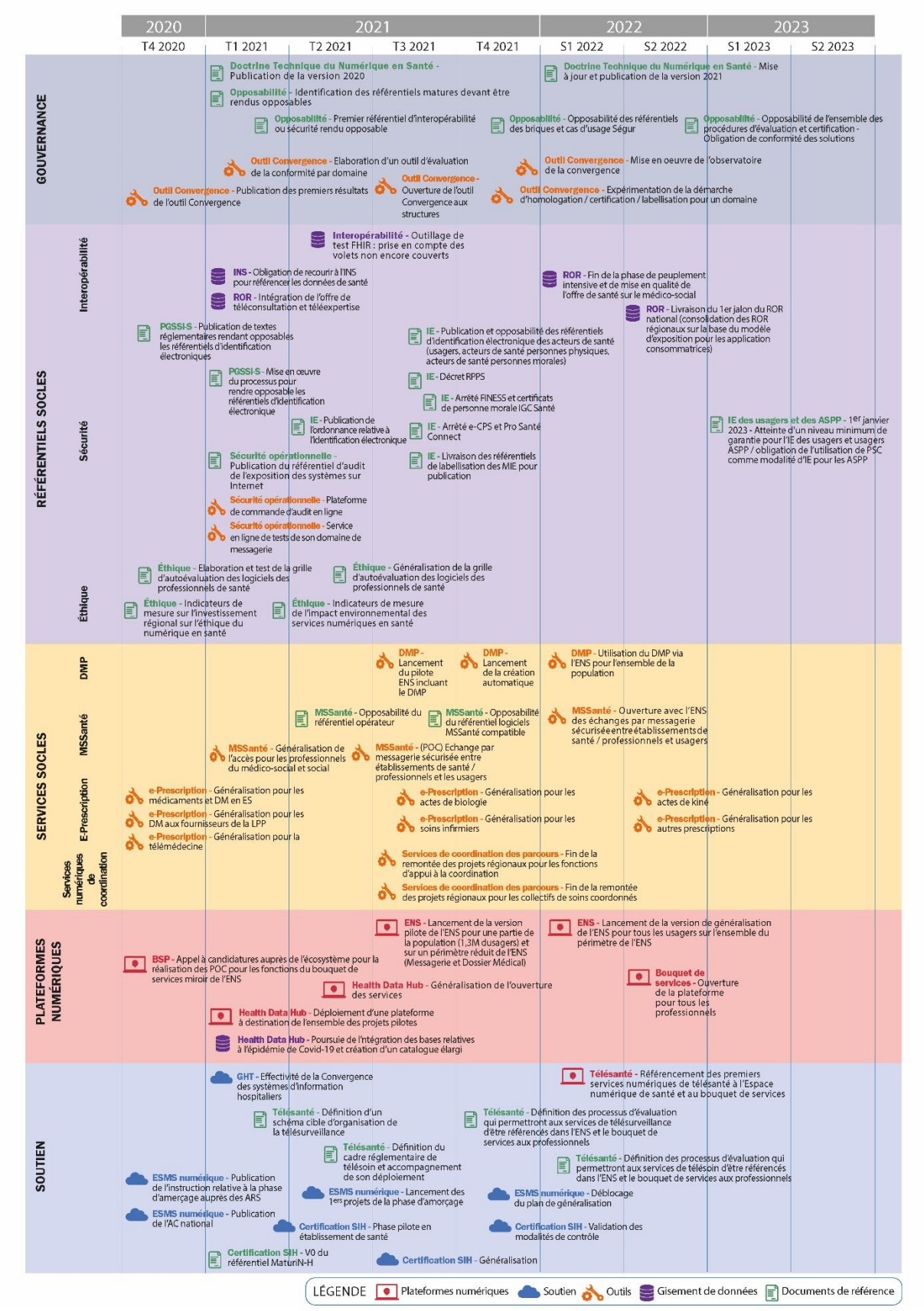
- Pour permettre aux promoteurs de services numériques de vérifier la conformité des services aux principes d'urbanisation, de sécurité et d'interopérabilité décrits dans cette doctrine technique, l'Etat met à disposition un espace de tests d'interopérabilité et un outil web d'auto-évaluation appelé *Convergence* ;
- L'outil web d'auto-évaluation *Convergence* facilite l'identification des actions à mener pour corriger les écarts et assurer la convergence à la cible attendue.
    - Des attestations de conformité seront à télécharger au sein de l'outil. Des contrôles aléatoires de vérification pourront être prévus par les services de l'Etat ;
    - Les résultats des tests de conformité à la doctrine feront l'objet d'une publication publique ;
    - Après le périmètre des services régionaux et des solutions industrielles, la démarche de convergence est étendue aux structures afin qu'elles puissent également évaluer leur maturité par rapport aux actions de la feuille de route du numérique en santé.
    - L'extension aux services nationaux fera l'objet de la dernière phase d'extension de périmètre de la démarche convergence.

- L'espace de tests d'interopérabilité est mis à disposition des industriels courant 2020. Cet espace permet de vérifier la capacité des services numériques à assurer l'interopérabilité de leurs documents et données de santé. Les résultats des tests menés sur l'espace seront publiés pour permettre aux utilisateurs finaux de vérifier le niveau d'interopérabilité de leurs solutions.

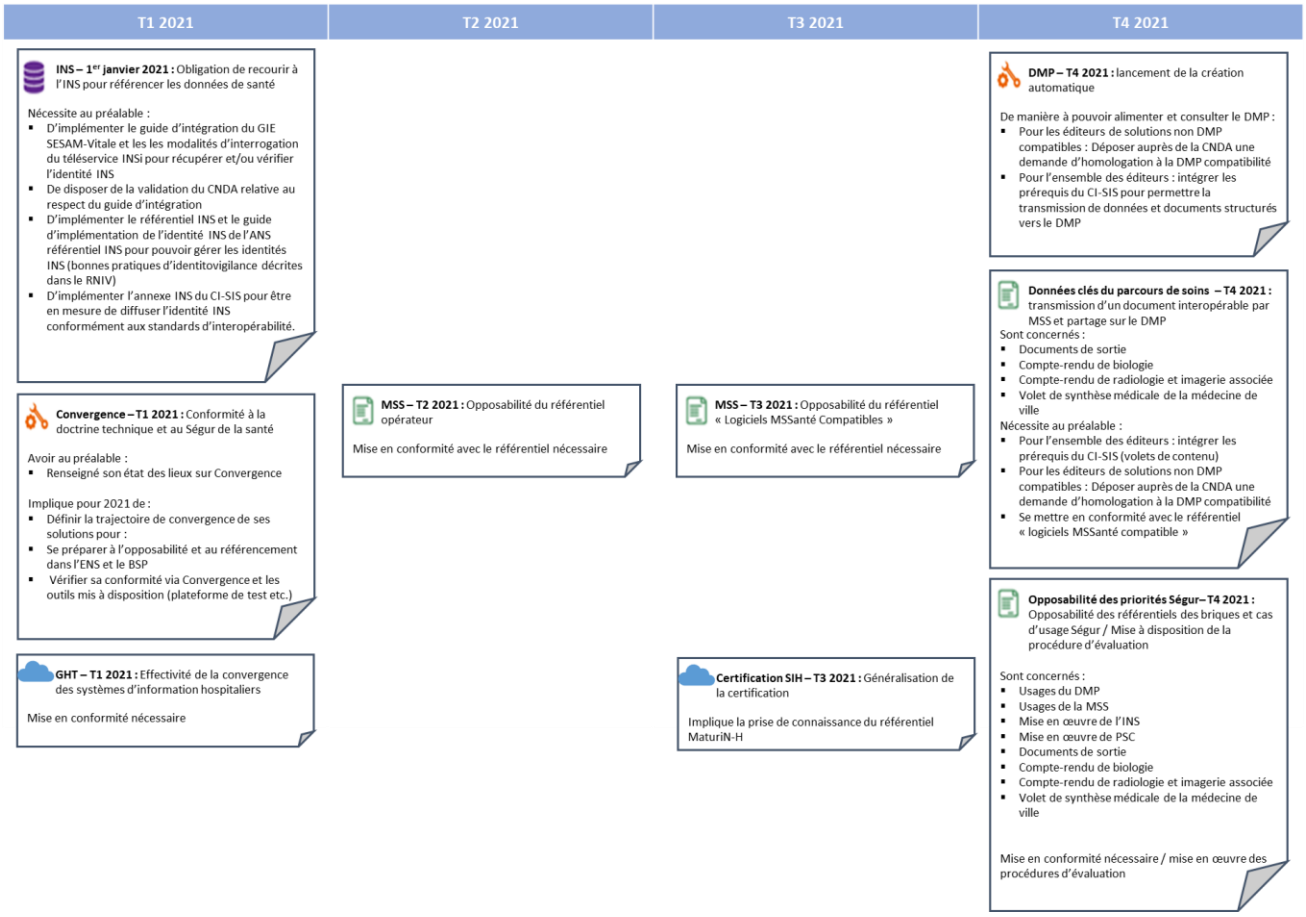
24. Les financements publics de services numériques de santé et le référencement des solutions dans les plateformes numériques de santé seront conditionnés au respect des règles contenues dans la doctrine technique :

- Les financements publics seront conditionnés à l'utilisation de services numériques conformes à la doctrine technique ;
- Le référencement des services numériques, publics comme privés, dans les plateformes numériques de santé impose la conformité à la doctrine technique.

MACRO-PLANNING RECAPITULATIF



FEUILLE DE ROUTE DES PRIORITES 2021



PRESENTATION DE LA DEMARCHE D'OPPOSABILITE

Les acteurs du numérique en santé s'engagent aux côtés des pouvoirs publics autour de la doctrine technique du numérique en santé et participent activement à l'élaboration et/ou la mise en œuvre de référentiels d'interopérabilité et de sécurité. Ces référentiels ont vocation à être rendus opposables, tout comme les procédures d'évaluation et de certification permettant de mesurer la conformité des systèmes d'information ou des services ou outils numériques.

Sur le plan réglementaire, cette démarche s'appuie sur les textes suivants :

- **L'article L 1110-4-1** qui permet de rendre opposable par arrêté la conformité à des référentiels d'interopérabilité ou de sécurité et qui peut aussi être appelé par différents textes réglementaires afin de spécifier le respect des référentiels opposables ;
- **L'article L 1110-4-2**, qui, sur la base exclusive des référentiels d'interopérabilité rendus opposables via le L. 1110-4-1, permet de :
  - Définir des procédures de vérification de conformité, en spécifiant les acteurs et référentiels cibles ;
  - Conditionner différents financements à l'atteinte du niveau de conformité.
- Potentiellement, **d'autres textes réglementaires** qui peuvent rendre opposables des référentiels. Par exemple :
  - **Arrêté du 24 décembre 2019 portant approbation du référentiel « Identifiant national de santé » ;**
  - **Article R 6211-4,** pour la transmission du "compte-rendu des examens de biologie médicale [qui] est structuré conformément au référentiel d'interopérabilité dénommé « volet compte rendu d'examens de biologie médicale ».

Cette démarche d'opposabilité est portée par les différents chantiers identifiés dans la doctrine technique du numérique en santé. Elle a vocation à faire partie des différents outils permettant de maitriser collectivement la trajectoire globale de mise en œuvre de la feuille de route, en s'appuyant sur trois piliers :

- **Une vision partagée**, globale, centralisée et cohérente de la trajectoire, des étapes et objectifs, en application directe de la doctrine technique du numérique en santé ;
- **La concertation**, inscrite dans l'article L 1110-4-1, permettant de s'assurer collectivement que les référentiels définis répondent aux cas d'usage et seront déployés ;
- **Une démarche progressive, sur plusieurs axes :** au niveau de chaque référentiel qui est appelé à être régulièrement mis à jour en fonction des contraintes et des retours d'expérience, mais aussi au niveau du "type" de référentiels, en partant de référentiels plutôt techniques vers des référentiels "fonctionnels" traitant des cas d'usage de bout en bout.

Les premières étapes de la démarche d'opposabilité consistent à :

- Effectuer un bilan partagé de la situation concernant les textes réglementaires, les dispositifs de contrôle existants, les référentiels établis ;
- Etablir un *modus operandi* de l'opposabilité d'un référentiel ;
- Déterminer les référentiels qui seront rendus opposables "au plus vite" ;
- Détailler et consolider les travaux d'opposabilité pour les briques et cas d'usage SEGUR et le calendrier associé, en lien étroit avec les travaux SEGUR.

Concernant la comitologie de cette démarche d'opposabilité, il convient de souligner qu'elle doit être portée à part entière au niveau de chaque brique / chantier de la feuille de route du numérique en santé par l'ensemble des acteurs concernés. Des comités de pilotage spécifiques "opposabilité" avec les différents acteurs, et en particulier avec les fédérations d'industriels ont vocation à :

- Consolider une vision de synthèse globale sur la trajectoire d'opposabilité des référentiels et la mise en œuvre des procédures de vérification associées à ces référentiels ;
- Intégrer les priorités de politique publique et garantir ainsi la cohérence globale des chantiers en lien avec la capacité à faire de l'ensemble de l'écosystème.

Un premier travail d'analyse a permis de faire émerger une première synthèse retranscrite ci-dessous. Chaque élément est évalué suivant une échelle à quatre niveaux :

- ✗ : Inexistant ou très insuffisant
- ! : Quelques éléments, insuffisants ou avec des limitations importantes
- ✓ : Défini, mais avec quelques manques / limitations
- ✓ : Défini et satisfaisant

Analyse		MS Santé Opérateur	MS Santé Client	DMP	INS	PSC	DUI	Production			Consommation / intégration		
								CR Bio	VSM	IDL	CR Bio	VSM	IDL
Définition de la brique	Couverture juridique de la brique eSanté	!	!	✓	✓	✗	✓	✓	!	✓	!	✗	✓
	Référentiels techniques	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Référentiels fonctionnels, "cas d'usage"		✓	✗	✓	✗	✓	✓	✓	✓	!	!	!
	Convergence		✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Tests et contrôles existants	Plateforme de tests / intégration	✓	✓	✓	✓	✓	✗	✓	✓	✓	!	!	!
	Procédures de vérification / référentiels techniques	✓	!	✓	✓	✓	!	✓	✓	✓	✗	✗	✗
	Procédures de vérification / référentiels fonctionnels	✗	✗	✗	✗	✗	!				✗	✗	✗
	Publication de listes d'acteurs/solutions compatibles	✓	✓	✓	✓	✓	!	!	!	!	✗	✗	✗
Opposabilité	Texte réglementaire rendant opposable l'utilisation de la brique	✗	✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓
	Texte réglementaire définissant les modalités de vérification de conformité	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗

TRAJECTOIRE

1. Rendre opposables en déclinaison de l'article L 1110-4-1 les référentiels des briques et cas d'usage du SEGUR
2. Rendre opposables en déclinaison de l'article L 1110-4-2 les procédures d'évaluation et de certification et publier les solutions conformes à ces référentiels

SYNTHESE DES ACTIONS CLES

Actions	Echéances
Rendre opposable en déclinaison de l'article L. 1110-4-1 un premier référentiel	Mars 2021
Réaliser une enquête « opposabilité » sur l'identification des référentiels matures, i.e. dont l'opposabilité devrait être priorisée, et sur la priorisation des travaux sur les référentiels à mettre à jour ou à rédiger	Premier trimestre 2021
Rendre opposables en déclinaison de l'article L 1110-4-1 les référentiels des briques et cas d'usage du SEGUR	Fin 2021
Rendre opposable en déclinaison de l'article L 1110-4-2 la première procédure d'évaluation et de certification	Fin 2021
Disposer d'une procédure d'évaluation sur l'ensemble des référentiels et des cas d'usage SEGUR	Fin 2021
Rendre opposables en déclinaison de l'article L 1110-4-2 les procédures d'évaluation et de certification et publier les solutions conformes à ces référentiels	2022

SCHEMA D'ARCHITECTURE CIBLE

Dans la philosophie prônée par la feuille de route « accélérer le virage numérique », l'Etat se recentre dans un rôle **d'Etat plateforme** fixant des règles et mettant à disposition de la société civile et des acteurs privés des ressources, en leur laissant la liberté de proposer des services numériques à l'aide de ces ressources. Il y gagne ainsi en **agilité**, permettant aux citoyens et aux professionnels du secteur de la santé et du médico-social de bénéficier rapidement de services innovants, et en **souveraineté** en fixant les règles en matière d'urbanisation, d'interopérabilité, de sécurité ou encore d'éthique.

L'Etat fournit ainsi le cadre d'actions au sein duquel les **acteurs publics et privés peuvent proposer des solutions numériques innovantes** pour les professionnels et les usagers du système de santé.

Le schéma d'architecture ci-dessous précise ce cadre.

Dans ce schéma, l'**Etat intervient à quatre niveaux** :

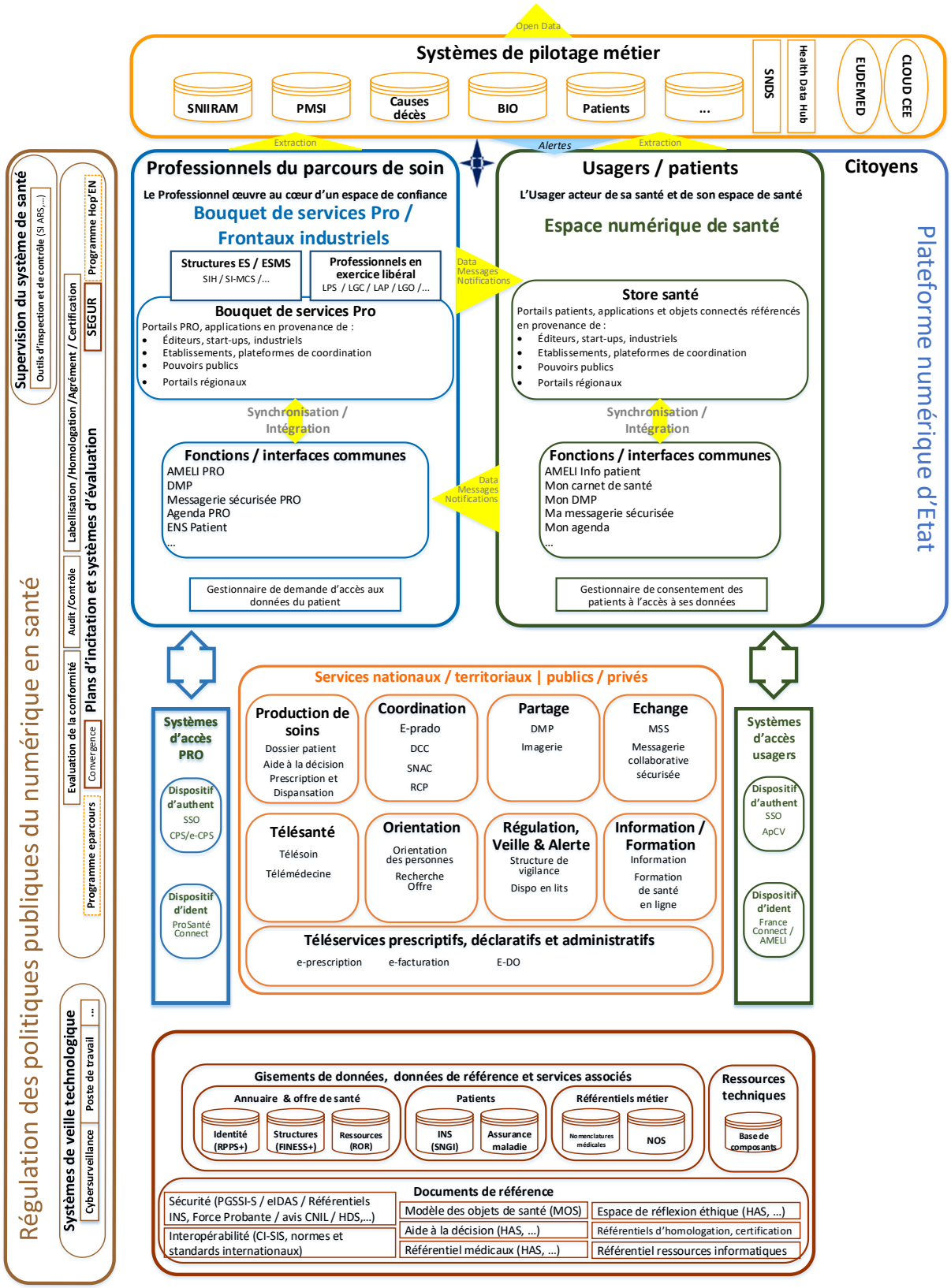
1. **L'Etat définit les règles et les bonnes pratiques, en matière d'éthique, de sécurité et d'interopérabilité**, indispensables pour faciliter le partage et l'échange de données de santé en toute confiance. Ces règles et bonnes pratiques seront rendues publiques, au travers de documents de référence publiés sur le site esante.gouv.fr, dont certains ont vocation à être rendus opposables.

2. **L'Etat, dans une logique d'open data, fournit les gisements de données de référence qui nourrissent les solutions numériques**. Il assure la qualité de ces données (pertinence, fraîcheur etc.), il facilite leur exploitation par les acteurs et s'assure du respect des différentes contraintes inhérentes au domaine de la santé (confidentialité des données, propriété intellectuelle etc.).

3. **L'Etat intensifie le déploiement de services socles** indispensables au bon fonctionnement du parcours de santé des usagers :
   - Le Dossier Médical Partagé (DMP), pour le partage des données de santé entre professionnels d'une part avec le BSP, et entre le patient et les professionnels qui le prennent en charge d'autre part avec l'ENS ;
   - L'espace de confiance de la Messagerie Sécurisée de Santé (MSSanté), pour l'échange de données de santé entre professionnels et entre professionnels et usagers par l'intégration de l'ENS dans cet espace de confiance MSS ;
   - La e-prescription, pour la transmission dématérialisée et sécurisée des prescriptions ; Les outils de coordination, pour faciliter l'organisation des parcours complexes
4. **L'Etat met à disposition trois plateformes numériques d'Etat :** l'Espace Numérique de Santé, à destination des usagers, le Bouquet de Services, à destination des professionnels, le Health Data Hub, pour l'exploitation des données de santé mutualisées et financées sur fonds publics. Ces plateformes constituent un « contenant » dans lesquelles seront proposées les solutions numériques portées par les acteurs publics et privés. Ces plateformes facilitent l'accès aux multiples solutions numériques dont un utilisateur (usagers ou professionnels) peut avoir besoin. Elles garantissent également que les solutions qui y seront référencées respectent les règles fixées par l'Etat en matière d'éthique, de sécurité et d'interopérabilité.

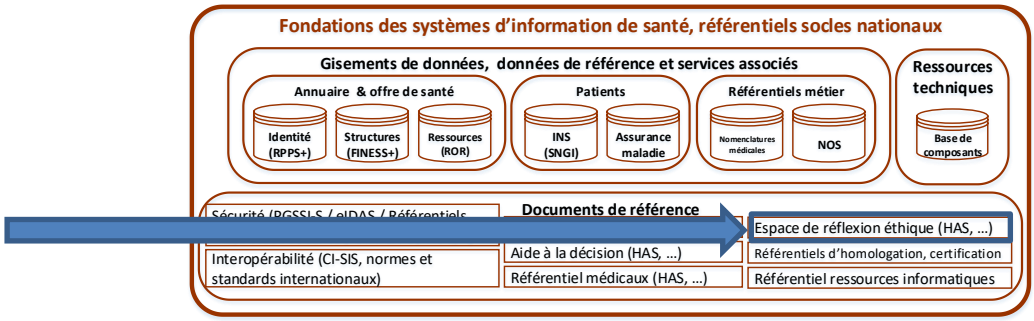
5. **L'Etat s'assure de la cohérence de la feuille de route nationale avec la feuille de route e-santé européenne** : l'Etat s'assure que l'architecture cible et sa trajectoire sont cohérentes avec les attentes, engagements et obligations de la France au regard de son implication dans la feuille de route e-santé européenne.

CIBLE DE L'URBANISATION SANITAIRE ET MÉDICO-SOCIALE



REFERENTIELS SOCLES

1 – Cellule Éthique du Numérique en Santé



DOCTRINE

❶ Constat

Entre confidentialité, pour garantir le secret médical, et ouverture, échange et partage, pour améliorer la qualité des soins et permettre la création de connaissances et la promotion de la recherche, les données de santé et leur traitement interrogent aujourd'hui la médecine d'Hippocrate. Les usages du numérique en santé peuvent en effet rapidement constituer une source d'inquiétude pour les utilisateurs (qu'ils soient professionnels de santé ou patients) en ce qui concerne l'utilisation des données et des services associés. Il est donc essentiel d'assoir le renforcement du virage numérique en santé sur un cadre de valeurs et un référentiel d'éthique afin de structurer les usages et de fixer des limites quant à l'utilisation des données et des services. Ce cadre éthique doit permettre de donner du sens au déploiement de la e-santé en France, en développant la confiance des usagers et des professionnels de santé.

Les quatre piliers de l'éthique que sont **l'autonomie, la bienfaisance, la non-malfaisance et la justice** sont traditionnellement intégrés dans les différents codes de déontologie en santé, notamment dans le code de déontologie médicale. Appliqués à l'éthique du numérique en santé, ces piliers doivent ainsi concerner **l'éthique des données, des algorithmes, des systèmes, des pratiques et des décisions** (cf. intelligence artificielle). Si le RGPD (règlement général de protection des données) est nécessaire pour pouvoir garantir une conformité éthique en matière de données et d'algorithmes, il n'est pas suffisant pour couvrir toutes les dimensions de l'éthique du numérique en santé.

Une autre dimension de l'éthique du numérique en santé devra également concerner les préoccupations quant à la réduction des impacts environnementaux. Le développement des projets numériques en santé doit ainsi désormais intégrer un volet environnemental (via des démarches d'écoconception) en accord avec la Stratégie Nationale Bas-Carbone[8], réaffirmée dans la feuille de route du gouvernement pour réduire l'empreinte environnementale du numérique publiée le 8 Octobre 2020.

La volonté de la France est également de proposer cette approche au niveau européen et international.

[8] https://www.ecologie.gouv.fr/sites/default/files/2020-03-25_MTES_SNBC2.pdf

❷ Proposition / objectifs

Il est donc proposé de définir et d'assurer le portage d'un cadre éthique qui intègre la totalité des dimensions de l'éthique et l'ensemble des acteurs de l'écosystème de la e-santé, que ce soient les citoyens, les professionnels de santé (ayant une pratique en établissements de santé ou en ville), ou les industriels (fabricants et éditeurs) :

- Il s'agit d'élaborer un référentiel de labellisation ou de certification éthique des outils numériques, que ce soient des services à destination des professionnels de santé, ou des applis mobiles notamment à destination des citoyens (dans la perspective du référencement pour les plateformes « bouquet de services » et « espace numérique de santé ») ;
- Les travaux porteront dès l'amont avec une volonté d'engager les startups, et les éditeurs dans l'intégration d'une dimension éthique dès la conception de solutions d'intelligence artificielle en santé (principe de l'éthique « *by design* »). L'objectif est de définir un guide de bonnes pratiques à destination des startups et des éditeurs allant dans ce sens ;
- Il s'agit également de construire une base d'outils pratiques de type « grilles de questionnement éthique en e-santé », afin d'aider les usagers et les professionnels dans leur compréhension des enjeux associés, et dans leur implication dans l'auto-évaluation éthique de leurs outils (notamment l'auto-évaluation des systèmes d'information hospitaliers (SIH) et des logiciels des professionnels de santé (LPS)) ;
- Par ailleurs, la société évoluant, il conviendra de relire le code de déontologie médicale afin de vérifier l'impact du numérique en santé sur les articles et les commentaires du code et de proposer des modifications pour aller vers un « code de e-déontologie » médicale ; Un travail équivalent sera réalisé sur les codes de déontologie des professions de santé à ordre.
- Enfin, un objectif sera d'initier une démarche visant à réduire les impacts environnementaux, et notamment les émissions de gaz à effet de serre, des outils et services numériques en santé en créant un référentiel de méthodes et d'analyse d'écoconception (optimiser la solution informatique et toutes ses composantes logicielles et matérielles pour qu'elle sollicite moins de ressources tout au long de son cycle de vie, de sa conception à son décommissionnement) destiné aux porteurs et acteurs des projets numériques de santé.

Afin de mesurer la progression de chacune de ces actions, des indicateurs de performance sont définis. L'objectif est d'organiser le partage des initiatives gagnantes entre les régions et d'accompagner globalement l'ensemble des régions afin qu'elles puissent atteindre un niveau maximal.

❸ Cible

Représentants des usagers, éditeurs de LPS et de SIH, startups, développeurs d'applis mobiles de santé, fabricants d'objets connectés, universitaires de l'éthique et chercheurs.

TRAJECTOIRE

Action	Jalon
Création de la cellule éthique du numérique en santé du Conseil du Numérique en Santé.	Effectué au T3 2019
Organisation des GT en charge des différents travaux.	En continu depuis T3 2019
Élaboration d'une grille permettant une auto-évaluation des systèmes d'information hospitaliers, mise en œuvre sur une plateforme nationale, test sur un échantillon d'établissements de santé (T1 2020), généralisation (T2 2020), analyse des résultats (T3 2020).	Courant 2020 (fait sur un échantillon, retard sur la généralisation)
Élaboration d'une grille permettant une auto-évaluation des logiciels des professionnels de santé, test sur un échantillon de logiciels (T4 2020), généralisation (T2 2021), analyse des résultats (T3 2021).	En cours
Conception, mise en œuvre et diffusion d'un film de sensibilisation du grand public au sujet de l'éthique du numérique en santé.	Effectué au T3 2020
Élaboration d'un référentiel de bonnes pratiques pour inscrire la démarche de conception d'une solution d'IA dans un principe d'éthique « by design » (en ce qui concerne les systèmes d'intelligence artificielle)	Effectué au T4 2020
Actualisation du code de déontologie médicale et propositions d'évolution vers un code de e-déontologie médicale.	A planifier (initialement prévu en 2020, reporté, travail sur le code de déontologie du CNOP)
Cartographie des initiatives régionales en éthique du numérique de santé	A planifier (initialement prévu en 2020 et reporté du fait de l'annulation des journées régionales d'éthique et de la crise sanitaire en cours)
Proposition d'indicateurs permettant de mesurer l'investissement régional sur le sujet de l'éthique du numérique en santé et de suivre son évolution au cours du temps, mise en œuvre d'actions ciblées si nécessaire.	En continu à partir de T4 2020
Proposition d'indicateurs de mesure de l'impact environnemental des services numériques en santé.	T4 2020 - T1 2021

2 – Urbanisation des systèmes d'information de santé

Pour assurer la cohérence de l'ensemble des systèmes d'informations de santé, il est indispensable de définir et d'appliquer un certain nombre de principes d'urbanisation.

DOCTRINE

Des premiers principes ont été exposés dans l'instruction n° SG/DSSIS/2016/147 du 11 mai 2016 relative au cadre commun des projets d'e-santé[9].

Le cadre d'urbanisation sectoriel des SI de santé, vise à dépasser cette première brique et à décliner pour les SI de santé, les règles d'urbanisation des SI, issues du cadre d'urbanisation européen et du cadre d'urbanisation des SI de l'état.

L'Etat confie à l'ANS l'élaboration et la publication d'un cadre d'urbanisation sectoriel qui précise et complète ces règles.

Extrait des principes du cadre d'urbanisation sectoriel :

- **Principes généraux :**
  - **GS1** : toute action de création ou de transformation de SI doit être conforme au cadre réglementaire ainsi qu'à la politique de sécurité applicable aux SI de santé (et notamment le RGPD et procédure CNIL) ;
  - **GS2** : toute action de création ou de transformation de SI doit être portée par un usage.
  - **GS3** : toute action de création ou de transformation de SI doit favoriser directement ou indirectement le meilleur parcours de santé au bénéfice de la personne prise en charge.
  - **GS4 :** toute décision de transformation ou création de SI doit être éclairée par la recherche systématique d'un retour d'expérience sur un besoin équivalent.
  - **GS5 :** l'usage des services, applications, composants et infrastructures, construits pour l'ensemble du secteur doit être privilégié.
  - **GS6** : procéder systématiquement au cadrage juridique du projet.

- **Principes de Gestion des données :**
  - **DS1 :** les données de référence doivent être gérées avec une gouvernance clairement établie.
  - **DS2 :** les données échangées entre SI doivent être formalisées, définies sur la base d'un vocabulaire commun, contextualisées et combinables les unes aux autres.
  - **DS3 :** les données de référence doivent être facilement réutilisables, partageables et accessibles.

[9] Le cadre commun des projets de e-santé publié en 2016 précise les référentiels applicables, le socle commun minimum de services à mettre en œuvre dans l'ensemble des territoires, et les principes de conduite de projets de e-santé : https://esante.gouv.fr/actus/politique-publique/publication-de-l-instruction-relative-au-cadre-commun-des-projets-de-e

- **Principes de conception générale des systèmes d'information :**
  - **CS1** : la réutilisation, la mutualisation, voire l'intégration et/ou l'achat des solutions disponibles (logiciels libres ou logiciels du marché) doit être privilégiée.
  - **CS2** : les flux d'échange entre les SI doivent être conformes aux orientations nationales en termes d'interopérabilité.
  - **CS3** : les adhérences entre les SI doivent être réduites.
  - **CS4 :** un utilisateur doit pouvoir accéder à un système d'information partagé tout en restant dans le contexte de son environnement informatique.
  - **CS5 :** dans la mesure du possible et dans le respect de la législation en vigueur, il ne doit être demandé qu'une seule fois aux utilisateurs des systèmes d'information de fournir des informations, et seules les informations pertinentes doivent être demandées.

- **Principes d'évaluation :**
  - Tous les services ou projets doivent faire l'objet d'une évaluation quant à leur importance et s'aligner, le cas échéant, en convergeant pour atteindre le niveau de conformité opérationnelle requis et en cohésion aux principes d'urbanisation sectorielle

TRAJECTOIRE

Mise en œuvre et construction des SI de santé urbanisés :

- Ces principes sont mis en œuvre dans les services socles et les référentiels nationaux du socle du système de santé et du médico-social ;
- Les services métier proposés notamment via l'espace numérique de santé et/ou le bouquet de services professionnels de santé.

Les services socles et les référentiels nationaux sont directement utilisés par les unités de production (sans passer par des services applicatifs proxy). Leur conception et leur développement est piloté par l'Etat.

Les services métier ont vocation à alimenter le catalogue de services métier disponible au niveau national notamment via l'ENS et/ou le bouquet de services professionnels. Ils sont, au préalable, expérimentés par des acteurs publics et/ou industriels identifiés[10] qui les conçoivent, les réalisent et les testent sur un périmètre régional.

[10] L'attribution aux différents acteurs des services métiers à expérimenter ainsi que la généralisation et ses modalités en fin d'expérimentation sont décidés en Comité ARS. Le Comité ARS regroupe les membres des comités de direction d'ARS en charge des sujets de santé numérique et les DG référents pour le numérique. Il est piloté par la DNS.

SYNTHESE DES ACTIONS CLES

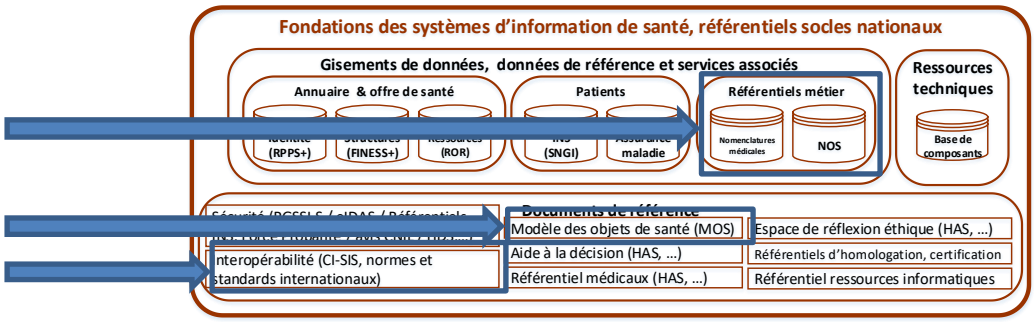
Le tableau ci-après présente une vue synthétique des actions et les échéances associées.

Action	Jalon
Publication du cadre d'urbanisation sectoriel et de ses annexes	Effectuée en novembre 2019

POUR EN SAVOIR PLUS

- The New European Interoperability Framework
  - https://ec.europa.eu/isa2/eif_en
- Cadre commun d'urbanisation du système d'information de l'Etat
  - http://references.modernisation.gouv.fr/urbanisation-du-systeme-dinformation-de-letat
- Cadre d'urbanisation sectoriel disponible sur le site de l'Agence du numérique en santé :
  - https://esante.gouv.fr/sites/default/files/media_entity/documents/%5Basip%5D%5Bcuss%5D-doctrine-urbanisation-sectorielle-sante-v0.15.pdf

3 - Interopérabilité des systèmes d'information de santé



L'interopérabilité est le garant de l'échange et du partage d'informations entre deux systèmes n'ayant pas forcément la même finalité. Elle permet leur traitement de manière efficiente et pertinente. Le contraire de l'interopérabilité est le système fermé ou propriétaire qui ne permet aucun échange fluide sans travaux de transcodage préalable. L'interopérabilité se divise en :

- **Interopérabilité « technique »** c'est-à-dire **l'interconnexion** entre deux systèmes, s'appuyant sur **l'utilisation d'interfaces définies, de normes et de protocoles partagés** dans le respect des exigences de sécurité et de confidentialité des données personnelles de santé.
- **Interopérabilité « sémantique »** est **basée sur des référentiels d'interopérabilité**, permettant à deux systèmes d'utiliser un langage commun (mots et syntaxe) pour produire et exploiter les données de santé échangées. C'est sur ces bases sémantique et syntaxique que les industriels développent des services à valeur ajoutée en retravaillant les données (courbes d'évolution temporelle, aide à la décision, traitement automatique du langage naturel, intelligence artificielle par exemple).

DOCTRINE

L'Etat définit la Doctrine qui porte le pilotage stratégique de l'interopérabilité « technique » et « sémantique » des systèmes d'information de santé.

❶ L'Etat rappelle les grands principes généraux de la doctrine de l'interopérabilité :

L'ensemble des spécifications d'interopérabilité (au sein du Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS)) et des terminologies constitue un **bien commun,** qui respecte le principe de transparence, de collaboration, de participation et d'éthique.

Les principes généraux de la doctrine d'interopérabilité :

- **Principe de transparence**
  - Livrables en OpenData, licence ouverte ETALAB (LOV2), données 5 étoiles[11]
  - Equité de traitement entre les industriels
- **Principe de collaboration**
  - Concertation des livrables
  - Transversalité des expertises
- **Principes de participation**
  - Co-construction des livrables avec l'écosystème
  - Evaluation des actions et des livrables
- **Principes éthiques**
  - Respect du cadre juridique
  - Respect des droits des patients et des usagers
  - Equité de traitement entre les acteurs

❷ L'Etat confie à l'ANS le soin d'organiser la représentation de la France auprès des instances internationales de l'interopérabilité et de normalisation

L'ANS est en charge de l'organisation de la représentation de la France dans les instances internationales de l'interopérabilité et de normalisation.

Interop'santé, association à laquelle l'ANS est adhérente, représente la France dans l'organisation internationale Integrating the Healthcare Enteprise (IHE) qui a vocation à produire des spécifications d'interopérabilité pour développer le partage de données de santé et dans l'organisation mondiale de standardisation HL7.

L'ANS souhaite renforcer la participation au sein d'HL7[12] et participer aux GT interopérabilité eHealth network (technical and semantics).

Préalablement à la réactivation du Groupe Numérique et Santé, l'ANS réalisera avec l'aide de l'AFNOR une cartographie des travaux de normalisation internationale en informatique de santé qui permettra de sélectionner avec les acteurs de l'écosystème (industriels…) les commissions, instances… de normalisation au niveau international (CEN, ISO) que les acteurs français doivent suivre.

[11] https://5stardata.info/fr/ : OpenData5étoiles : programme de déploiement du partage de données en 5 niveaux, identifiés par des étoiles. « Cinq étoiles » définit l'étape d'ouverture maximale des données, correspondant à la licence ouverte LOV2.

[12] https://www.hl7.org/

❸ Pour intensifier le partage et l'échange des données de santé entre solutions, l'Etat confie à l'ANS la responsabilité de l'élaboration et de la publication des référentiels d'interopérabilité[13] lisibles, enrichis et maintenus qui se composent :

- De **spécifications d'interopérabilité[14]**; Ces spécifications sont publiées sous forme de **volets** dans **le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS)** et pointent vers les nomenclatures à utiliser directement ou sous la forme de jeux de valeurs adaptés au contexte.
- **Le CI-SIS est le premier utilisateur des terminologies du secteur santé-social** ou des jeux de valeurs élaborés par l'ANS ou produits par un tiers public ou privé, mais validé par l'ANS, afin de garantir l'interopérabilité.

Le **CI-SIS** existe depuis 2009. Contenant initialement les spécifications utiles au partage de documents de santé[15] puis à l'échange de données de santé[16], il s'enrichit depuis 2015 au fil de l'eau en fonction des cas d'usage métiers remontés par les projets[17] nationaux ou territoriaux, déposés auprès du guichet unique. Il contient une vingtaine de modèles de documents médicaux au standard Clinical Document Architecture (CDA) (synthèse médicale, compte-rendu de biologie, …).

Les spécifications contenues dans le CI-CIS :

- Concernent les **échanges d'information** entre composants de systèmes d'information (i.e. les flux) et ne portent pas sur le cœur des applications ;
- Sont fondées sur des **normes internationales** d'interopérabilité du secteur sanitaire cohérentes avec les feuilles de route industrielles, et **contextualisées par cas d'usage** (en priorité les **profils IHE**, à défaut **CDA**[18] pour les documents partagés ou échangés, ou **FHIR**[19] le cas échéant ; et étude au cas par cas lorsqu'aucune de ces trois normes n'est adaptée au cas d'usage) ou au contexte du projet porteur de l'usage ;
- Incluant les spécifications techniques des téléservices de l'Assurance maladie (CI-TLSi) depuis 2020,
- **Comprennent une partie modélisation métier** qui s'appuie sur des concepts indépendants de la norme d'interopérabilité utilisée ; cette modélisation peut s'appuyer sur des bibliothèques de concepts centralisant les définitions, le nommage, structures et codage des informations traitées notamment le modèle des objets de santé (MOS) pour les concepts non médicaux et pour les concepts médicaux les modèles de sections et d'entrée CDA et les ressources FHIR et OMOP[20] ;
- Sont **adaptées au contexte français** (cadre juridique, orientations d'urbanisation, services nationaux mutualisés, référentiels de sécurité…) ;

[13] L'article L1110-4-1 modifié par la loi de santé 2019 décrit ainsi les référentiels d'interopérabilité « Les référentiels d'interopérabilité … s'appuient sur des standards ouverts en vue de faciliter l'extraction, le partage et le traitement des données de santé dans le cadre de la coordination des parcours de soins, de l'amélioration de la qualité des soins et de l'efficience du système de santé ou à des fins de recherche clinique, chaque fois que le recours à ces standards est jugé pertinent et possible par le groupement d'intérêt public mentionné à l'article L. 1111-24 du présent code. »

[14] Documents de référence inscrit dans le schéma d'architecture

[15] Utilisées notamment pour les interfaces entre les logiciels des professionnels de santé et le DMP, et donc prises en compte dans le processus d'homologation à la DMP compatibilité.

[16] dans le cadre de la mise en place des messageries sécurisées de santé MSSanté

[17] à titre d'exemple, 4 volets ont été élaborés à la demande des porteurs de projet territoire de soins numérique (TSN) : gestion d'un agenda partagé, gestion des notifications, accès aux recommandations vaccinales, et gestion du « cahier de liaison ».

[18] CDA = Clinical Document Architecture, le standard CDA est profilé par cas d'usage par IHE, puis décliné en volets de contenu (modèles de documents médicaux) par l'ANS en France.

[19] FHIR = Fast Healthcare Interoperabilité Ressources, en cours de développement au sein d'HL7 (Health Level 7) et qui devrait être profilé par cas d'usage pour des interfaces parfaitement opérables.

[20] OMOP = Observational Medical Outcomes Partnership, modèle de données dont l'objectif est de faciliter l'exploitation des données de santé, https://www.ohdsi.org/data-standardization/

- Des **terminologies de santé du secteur santé-social**. Ces terminologies sont des **référentiels permettant le codage non ambigu d'une information.** Par « terminologie » sans autre précision, il faut entendre **ontologie, classification, nomenclature, terminologie, jeux de valeurs et alignements**, qu'on peut regrouper sous le vocable **ressources sémantiques**.

L'ANS crée en 2019, un **centre de gestion des terminologies de santé (CGTS)[21], guichet national public distribuant gratuitement** les **terminologies et autres ressources sémantiques**, en garantissant à tous les utilisateurs **l'égalité d'accès** à ces référentiels dans le **respect de la loi sur la République numérique**.

Ces ressources sémantiques sont rendues accessibles via un **serveur multi-terminologies (SMT)** dans un **format réutilisable** par les industriels pour l'intégration dans les logiciels de professionnels de santé et en **garantissant leur qualité** et leur **distribution sécurisée par une licence ouverte (LOV2)**.

Les terminologies de santé sont fournies au CGTS pour publication par **différentes structures (**appelées **unités de production)** qui **conservent la propriété intellectuelle** et **la responsabilité de leur maintenance**.

Le Codage et la structuration des données de santé, le traitement automatique du langage naturel, l'intelligence artificielle **s'appuient sur ces référentiels sémantiques sécurisés et partagés par tous.**

❹ L'Etat mène une politique volontariste pour faire appliquer les référentiels d'interopérabilité par :

Le renforcement au niveau législatif, dans la loi relative à l'organisation et à la transformation du système de santé de 2019, du caractère contraignant des référentiels :

- Nécessaire respect par les industriels des référentiels de sécurité et d'interopérabilité par les SI permettant **l'échange et le partage de données de santé à caractère personnel** (article L. 1110-4-1 du CSP).
- **Mise en place d'une nouvelle procédure de vérification de conformité pour renforcer l'effectivité des référentiels**[22] **:** Un décret en Conseil d'Etat prévoyant le cadre applicable aux procédures d'évaluation de la conformité d'un service/SI/outil aux référentiels d'interopérabilité est en cours de finalisation (art. L. 1110-4-2 I du CSP) – Objectif de publication : **avant fin 2020**.
- Un comité de pilotage animé par l'ANS et la DNS, associant l'ensemble des parties prenantes, est mis en place pour définir la trajectoire d'opposabilité des référentiels qui devront être adoptés par arrêté du ministre[23].

[21] Action 10 de la feuille de route stratégique du numérique en santé.

[22] La conformité d'un système d'information ou d'un service ou outil numérique en santé aux référentiels d'interopérabilité mentionnés à l'article L. 1110-4-1 est attestée dans le cadre d'une procédure d'évaluation et de certification qui doit être définie par décret en Conseil d'État. L'attribution de fonds publics dédiés au financement d'opérations relatives aux services ou outils numériques en santé sera conditionnée à des engagements de mise en conformité aux référentiels d'interopérabilité. L'Etat pourra prévoir des modalités complémentaires d'incitation à la mise en conformité par décret en Conseil d'État. Un dispositif d'entrée en vigueur progressif est prévu avec une date butoir fixée au 1er janvier 2023.

[23] Action 8 de la feuille de route stratégique du numérique en santé.

❺ Une nouvelle gouvernance de l'interopérabilité des SI de santé et du médico-social est mise en place.

Le rapport « Accélérer le virage numérique »[24] (septembre 2018) fixe dans ses préconisations de nouveaux objectifs à l'interopérabilité en France :

- Étendre les travaux sur l'interopérabilité en santé au médico-social et au social,
- Rendre opposables les référentiels d'interopérabilité dans une logique graduelle des exigences,
- Appliquer les exigences d'interopérabilité aux structures publiques,
- Répondre aux besoins d'interopérabilité de l'espace numérique de santé,
- Labelliser les logiciels médicaux et hospitaliers ouverts et interfaçables.

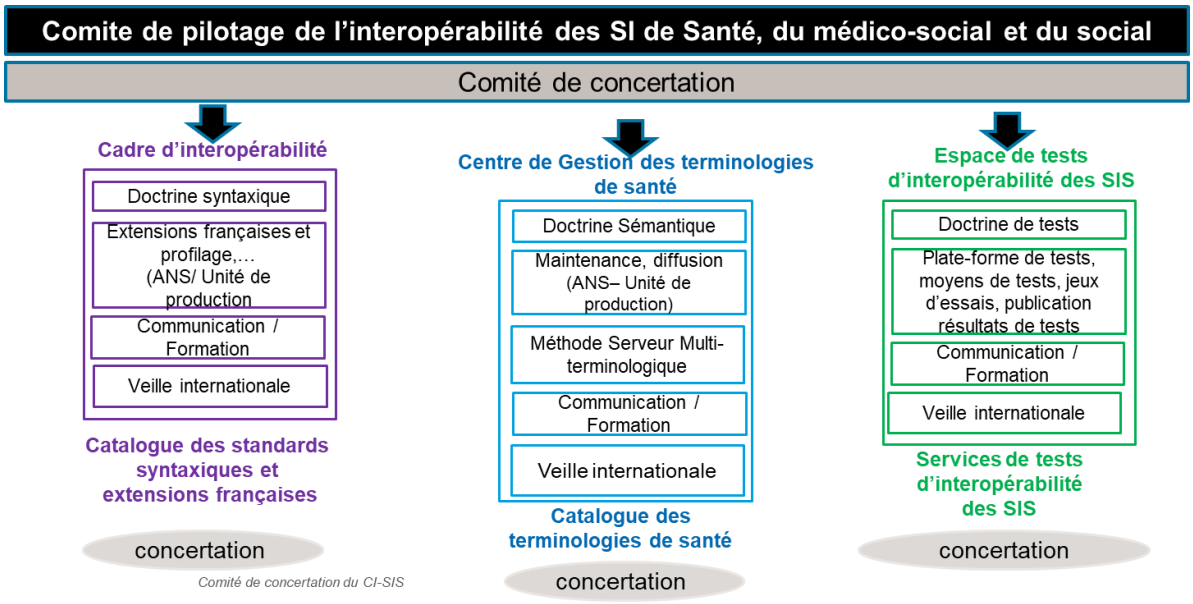
Ces nouveaux objectifs impliquent de **faire évoluer la gouvernance du Cadre d'Interopérabilité des SIS**. Cette nouvelle gouvernance doit aussi tenir compte des freins au déploiement sur le terrain des référentiels d'interopérabilité des SIS :

- Une approche de l'interopérabilité limitée à la production de spécification d'interopérabilité : faiblesse des moyens de tests d'interopérabilité, implication insuffisante des demandeurs de spécifications d'interopérabilité dans le déploiement des usages sur le terrain,
- Une identification et une mobilisation insuffisantes des ressources expertes françaises en interopérabilité des SIS pour mener des projets de dématérialisation de données de santé,
- Des incitations à l'échange de données de santé conformément au CI-SIS limitées à quelques cas d'usage (lettre de liaison, volet de synthèse médicale, …) ou non-alignées sur les cycles de développement des industriels.

La gouvernance du CI-SIS doit donc évoluer vers une gouvernance de l'interopérabilité afin de :

- Couvrir les **nouveaux besoins d'interopérabilité des systèmes de partage de données de santé** (DMP, ENS, logiciels métier, plateformes régionales, entrepôts …), et de **de nouveaux domaines** (santé-social, social, objets connectés, …)
- **Fédérer plus largement les expertises disponibles en France**,
- Mieux **aligner l'offre industrielle et les politiques publiques de développement des usages sur les besoins de dématérialisation des acteurs**,
- **Conduire** l**es projets de dématérialisation de bout en bout,** depuis la production des spécifications d'interopérabilité jusqu'à la formation et l'accompagnement des utilisateurs finaux,
- Mettre en place de **nouveaux services de l'ANS par la création du CGTS outillé d'un SMT** ;
- **Permettre l'interopérabilité des solutions de e-santé européennes** au fur et à mesure de leur déploiement.

[24] https://solidarites-sante.gouv.fr/IMG/pdf/masante2022_rapport_virage_numerique.pdf



Cette gouvernance vise à **laisser à l'Etat stratège les décisions et orientations des évolutions de la doctrine** tout en permettant **d'associer les acteurs du secteur** (industriels, promoteurs de services et utilisateurs) aux définitions du périmètre d'opposabilité des référentiels d'interopérabilité[25] et des trajectoires de mise en œuvre.

Cette nouvelle gouvernance est constituée :

- **D'un comité de pilotage**
  - Chargé de prioriser les expressions de besoins d'interopérabilité en santé, médico-social et social transmises à l'ANS et de vérifier dans une étape d'impact les conditions de succès du projet sont réunies (choix normatifs, ressources sémantiques (terminologies, …) et moyens de tests à mettre en œuvre pour les industriels, impact sur les solutions des éditeurs, moyens prévus en termes de conduite du changement et engagement du sponsor du projet, …). Mais également d'intégrer les attentes de la feuille de route européenne validée en France,
  -
  - Chargé de proposer **une trajectoire d'opposabilité** d'un référentiel d'interopérabilité pour publication de l'arrêté correspondant et **concevoir et coordonner les dispositifs** (AAP, programme national**) d'incitation des acteurs** (industriels, professionnels de santé, acteurs sociaux, …) à la mise en œuvre d'un référentiel d'interopérabilité avec le comité Territoires,
  - Présidé par la Direction du Numérique en Santé (DNS),
  - Et composé de l'Agence du Numérique en Santé (ANS), la Direction Générale de l'Organisation des Soins (DGOS) et la DGCS, la Caisse Nationale d'Assurance Maladie (Cnam), le GIE SESAM-VITALE, la Caisse Nationale de Solidarité et d'Autonomie (CNSA), la Haute Autorité de Santé (HAS), l'Agence de l'Appui à la Performance (ANAP) et le Health Data Hub,
- **D'un comité de concertation**
  - Pouvant effectuer des recommandations en termes de priorisation **des projets de dématérialisation** de données de santé sur la base des expressions de besoins et des études d'impacts,
  - Présidé par l'ANS,
  - Et composé des représentants des directions centrales, des ARS, de la Cnam, des fédérations d'industriels et des organisations représentatives des professionnels de

[25] Action 8 de la feuille de route stratégique du numérique en santé

santé, des acteurs du secteur santé social et des associations d'usagers du système de santé agréées.

- **De comités de suivi** en charge :
  - Du CI-SIS composé de l'ANS et de participants volontaires du comité de concertation pour mener des études normatives par exemple (choix de standards, gestion du versionning…),
  - Du CGTS composé de l'ANS, des unités de production ayant conventionné avec l'ANS et de participants volontaires du comité de concertation,
  - De l'Espace de tests d'interopérabilité regroupant l'ANS et des participants volontaires du comité de concertation,

Pour chaque projet de dématérialisation, **un chef de projet pilote avec l'appui du sponsor du projet** (organisation de professionnel de santé, …) est chargé de **la mise en œuvre sur le terrain de la dématérialisation** conformément au référentiel d'interopérabilité et à la trajectoire validée par le comité de pilotage.

TRAJECTOIRE

❶ Le CI-SIS

Portés par l'ANS, les **travaux d'évolution concernant le CI-SIS se déclinent sur sept axes** :

Axe 1 : Enrichissement du CI-SIS avec de nouveaux cas d'usage, issus de la gouvernance[26] en suivant la doctrine technique :

- Des documents médicaux en CDA :
  - Volet de synthèse médicale (VSM V2) - CDA
  - Compte rendu d'anatomo-cytopathologie - CDA
  - Plan personnalisé de coordination des soins - CDA
  - Compte-rendu d'imagerie - CDA
  - Traitements médicamenteux d'un patient - CDA
  - Circuit du dispositif médical : fiche produit - CDA
  - Carnet de santé de l'enfant - CDA
- Des flux applicatifs inter-SI en FHIR lorsque c'est adapté
  - Référence d'image en FHIR - FHIR
  - Demande d'examens d'imagerie (standard cible à évaluer)
  - Alimentation d'un entrepôt de données santé publique – FHIR
  - Gestion du cercle de soins d'une personne dans le domaine sanitaire, médico-social et social,
  - Aide à domicile personnes âgées et handicapées – (standard à évaluer)
  - Alimentation et consultation d'une base de mesures (interaction et profilage des mesures) - FHIR
  - Gestion des tâches - FHIR
  - Gestion mutualisée habilitations et consentement (standard à évaluer)
  - Publication d'un référentiel d'identité - FHIR
  - Dépôt de dossier et orientation dans le médico-social - FHIR

[26] Les priorités définies par le Comité de pilotage de l'interopérabilité des SIS sont en cours de concertation avec l'ensemble des parties prenantes du CI-SIS jusqu'à fin novembre 2020.

Axe 2 : Mise à jour des catalogues de concept de référence avec les concepts manipulés dans les cadres des nouveaux volets du CI-SIS

- Mise à jour du catalogue des concepts utilisés dans les volets CDA en fonction des nouvelles spécifications de documents produites
- Mise à jour du Modèle des Objets de Santé en fonction des nouvelles spécifications des couches service et transport.

Axe 3 : Outillage du CI-SIS

- Pour maintenir le catalogue des concepts utilisés dans les volets du CI-SIS basé du HL7 CDA, l'ANS dispose d'un outil de conception et de modélisation des volets du CI-SIS. Cet outil pourra à terme être ouvert à des unités de production de volets du CI-SIS externes à l'ANS et couvrira aussi les volets du CI-SIS basés sur HL7 FHIR.
- L'ANS met à disposition des industriels du secteur sanitaire, médico-social et social qui implémentent des spécifications d'interopérabilité dans leur produit et des maîtrises d'ouvrage qui déploient ces produits un Espace de tests d'interopérabilité des SIS27. Il leurs permet de :
  - Vérifier la conformité d'un produit à une spécification d'interopérabilité ;
  - De s'informer sur la conformité d'un produit à une spécification d'interopérabilité.
- Cet espace de tests accélère et simplifie l'implémentation d'une spécification d'interopérabilité par un industriel dans ses produits grâce à des services de tests accessibles en libre-service. En fiabilisant les tests de conformité, il améliore la qualité des données échangées entre les acteurs.
- Depuis octobre 2020, les industriels et les maîtrises d'ouvrage peuvent vérifier l'interopérabilité de leur produit pour 12 spécifications du CI-SIS basées sur HL7 CDA ou FHIR et aux spécifications du Répertoire Opérationnel des Ressources.
- Depuis novembre 2020, les services de tests de conformité aux spécifications maintenues par Interop'Santé (IHE PAM, Hprim santé, ressources FHIR profilées par IHE France) sont aussi accessibles dans cet Espace de tests d'interopérabilité.
- L'ANS organise depuis 2019 une fois par an à l'occasion de la Journée National des Industriels un projectathon multi-volets à l'occasion duquel les participants peuvent réaliser des tests d'interopérabilité de bout en bout entre producteurs et consommateurs de données. En 2020, le projectathon ANS a réuni 23 industriels.

Axe 4 : Convergence des spécifications d'interopérabilité nationales des secteurs sanitaire, médico-social et social

- Les couches de transport du CI-SIS utilisé par le DMP, celles du CI-TLSi (téléservices intégrés) utilisées par les téléservices inte-régimes de l'assurance maladie, et celles du Ci Partenaires utilisé par APCV et les AMO pour les échanges inter-régimes sont fondées sur les mêmes normes et standards. Un document d'orientation entre les cadres d'interopérabilité a été produit en 2020 pour permettre aux éditeurs d'identifier rapidement quel cadre est applicable à quel usage. **Des travaux pourront être lancés avec l'Assurance Maladie pour identifier un cible technologique commune à l'ensemble des nouveaux services** (qu'ils soient dans le périmètre du CI-SIS ou dans le périmètre du CI TLSi) ainsi que les modalités de convergence du CI-SIS et du CI TLSi vers cette cible dans la mesure du possible. Le CI Partenaire sera intégré à ces travaux dans un second temps.
- Pour assurer l'interopérabilité des systèmes d'information au-delà du secteur sanitaire et rationaliser les développements des services numériques qui s'adressent aux professionnels

[27] https://esante.gouv.fr/interoperabilite/espace-de-tests-dinteroperabilite

de différents secteurs, l'ANS **étudie la convergence des différents référentiels** et **formalise les conditions d'intégration dans le CI-SIS** (reprise directe de spécifications, travaux de convergence, reprise du cas d'usage et élaboration de nouvelles spécifications techniques…). C'est dans ce cadre, par exemple, que la trajectoire d'intégration des cas d'usage métier d'ESPPADOM[28] dans la cible du CI-SIS est à étudier, avec un point d'attention sur la faisabilité d'un passage aux standards internationaux pour les éditeurs du marché.

Axe 5 : Accompagnement et évaluation de l'implémentation des référentiels d'interopérabilité :

- Les **productions du CI-SIS doivent être déployées jusque dans les outils métier** des professionnels bénéficiaires ultimes de l'interopérabilité. Pour cela, **le sponsor de la demande au CI-SIS doit s'engager à mettre en œuvre des mesures d'accompagnement facilitant ce déploiement** (AAP, programme d'accompagnement des éditeurs et des professionnels de santé (PS)). Une mise à jour des formulaires d'expression de besoins en interopérabilité et des exigences pour couvrir l'étape de déploiement sera faite (2020).
- **Une doctrine doit être établie sur le rôle de relais que devraient prendre les Groupement Régionaux d'Appui au Développement de la e-Santé (GRADeS)** en régions pour assurer cet accompagnement. (2020)
- **L'implémentation des référentiels d'interopérabilité doit être évaluée**. Une réflexion doit avoir lieu à l'occasion du Programme « **Hôpital numérique ouvert sur son environnement »** (HOP'EN) et du programme ESMS numérique, sur l'opportunité d'organiser des tests d'interopérabilité progressifs permettant de délivrer à terme un **Label Interopérabilité du logiciel** comme l'ANS le fait pour le label e-santé Maisons et Centres de Santé (MCS) (2020-2021) ou le label SI commun MDPH dans le secteur médico-social.

Axe 7 : Participation aux travaux internationaux d'interopérabilité et aux travaux de normalisation

- L'ANS assure une présence au sein d'IHE.
- L'ANS propose sa **candidature à HL7** (2020).
- Compte-tenu des ressources limitées, une réflexion doit être conduite pour **sélectionner et missionner des tiers de confiance,** extérieurs à l'ANS pour assurer plus largement cette couverture internationale (2020).
- L'ANS a pris contact avec l'AFNOR en vue de réactiver le **Groupe numérique et santé** (2020)
- L'ANS et la DNS participent aux réflexions et projets dans le cadre du réseau eHealth Network et des actions européennes conjointes de eHealth Action.

[28] La spécification d'ESPPADOM concerne les échanges de données entre les conseils départementaux et les structures de l'aide à domicile.

❷ Le CGTS : Centre de gestion des terminologies du secteur santé social

- La mise en place du CGTS outillé d'un serveur multi-terminologies (SMT), ainsi que des services afférents, se déroulent sur 3 ans sur 2019-2020-2021, selon deux axes principaux de travail :

Axe 1 : Consolider les fondations

- **Le SEGUR de la santé va fortement mobiliser l'ensemble de l'écosystème sur les 18 prochains mois** (déploiement fin 2021 / 2022) par la mise en place des briques fondamentales de l'Etat-plateforme afin de permettre l'échange de données de santé entre PS et avec le citoyen : INS, PSC, généralisation du DMP et de la MSSanté…
- **La mise en œuvre de cas d'usages fonctionnels d'échange et partage de données de santé au profit du patient est une priorité pour le CGTS** (compte-rendu d'examens de biologie médicale, compte-rendu d'examens d'imagerie médicale avec accès aux images, lettres de liaison, volet de synthèse médicale…). En conséquence, **les changements technologiques majeurs, dont SNOMED CT, ne sont pas envisageables sur les 18 prochains mois du SEGUR.**
- **Pour répondre à ces objectifs du « Ségur », le CGTS doit en priorité axer ses travaux sur les terminologies utiles aux cas d'usages fonctionnels d'échange « Ségur » :**
    - **Consolider les actifs CGTS** (cf actions détaillées) et **pérenniser la nouvelle Gouvernance sémantique** intégrée à celle de l'interopérabilité.
    - **Mettre en qualité et publier un socle de terminologies** pour répondre aux cas d'usage du Ségur sur les domaines suivants : données médicales, actes, produits de santé, biologie, examen de radiologie, oncologie. Pour chacun de ces domaines, il s'agit d'identifier les terminologies à mettre œuvre, l'unité de production qui en aura la responsabilité.
    - **Consolider les travaux sur l'outillage** :
        - Poursuite du développement du SMT et des fonctionnalités nécessaires ;
        - Rédaction d'un référentiel / guide de bonnes pratiques quant à l'usage du SMT par les éditeurs (suivi des mises à jour, etc).
- **Afin de sécuriser la mise à disposition des terminologies de l'OMS, le CGTS intègrera le Centre Collaborateur OMS France** et publiera sur son SMT les terminologies de l'OMS (CIM 10, CIM 11, ICF et ICHI).

Axe 2 : poursuivre le développement d'un corpus sémantique cohérent

- **Etablir une cartographie opérationnelle des terminologies** d'intérêt par cas d'usage avec l'ensemble de acteurs de la e-santé.
- **Continuer les travaux sur la terminologie SNOMED CT :**
    - **Compte tenu des priorités définies par le Ségur, des objectifs en termes de planning et des conclusions du rapport « Faut-il adopter la SNOMED CT ? », les travaux sur SNOMED CT auront pour objectif dans les 18 prochains de faciliter l'expérimentation sur le terrain de la SNOMED CT en créant un environnement favorable.**
    - **Un travail d'échange et de négociation** avec SNOMED International est nécessaire pour **aplanir les difficultés juridiques** soulevées par l'étude. Compte tenu de l'enjeu en termes d'investissement pour tout l'écosystème, cette phase initiale ne doit pas être négligée. L'objectif est **d'apporter une sécurité juridique** aux utilisateurs souhaitant expérimenter la SNOMED CT en France.
    - Pour faciliter son expérimentation par le terrain, il sera également négocié **la mise à disposition d'une version française traduite qualifiée**, sachant que :

- Des traductions françaises[29] existent déjà, auxquelles contribuent la Belgique, le Canada, le Luxembourg, la Suisse, et la société PHAST
- Une **traduction** de l'ensemble des termes de la SNOMED CT par **des méthodes automatiques** (mais non revue par des professionnels de santé) a été réalisée par l'ANS dans le cadre de l'étude « Faut-il adopter la SNOMED CT ? », en lien avec l'Ecole Polytechnique. Un des enjeux consiste à **pouvoir publier cette traduction au bénéfice de l'écosystème de la e-santé**.

- **Réévaluer l'intérêt économique de la licence nationale.** L'ANS va mettre à jour le recensement des licences affiliées acquises par les différents utilisateurs afin d'évaluer l'état du déploiement de la SNOMED CT en France et l'intérêt économique de la licence nationale. **Dans le cas positif**, l'ANS en concertation avec les parties prenantes (industriels, MOA, établissements de santé, professionnels de santé…) planifiera l'intégration de SNOMED CT dans le catalogue des terminologies du CGTS:
  - Mise en place d'une Unité de Production SNOMED CT ;
  - Intégration de SNOMED CT au SMT ;
  - Participation à la gouvernance de Snomed International.

Actions détaillées

- **Action 1 : Mise à disposition des terminologies dans un format standardisé RDF/OWL via le SMT. Deux modules avec des améliorations fonctionnelles seront mis en production en 2021 :**
  - Module de publication des terminologies (novembre 2020)
  - Module de gestion des terminologies (mars-avril 2021)
  - Module d'import/export des terminologies (juillet 2021)
- **Action 2 : webinaires sur l'utilisation du SMT V1 et ateliers de spécification du SMT V2 (2021)**
- **Action 3 : Mise en qualité et au format des terminologies pour publication dans le SMT :**
  - LOINC (jeux de valeurs LOINC et Circuit de la biologie), CISP-2, ADICAP, Snomed3.5VF (2020)
  - CIM-10, CIM-11, CCAM, NCBI Taxonomy, Cladimed, Medicabase (2021), NOS
  - Puis publications régulières des terminologies selon la feuille de route concertée du CGTS/SMT
- **Action 4 : Mise à jour de la feuille de route du CGTS/SMT** (terminologies prioritaires à publier dans le SMT en 2021) **grâce à un sondage en ligne** pour déterminer les besoins de l'écosystème en terminologies (octobre 2020)
- **Action 5 :** l'ANS candidate pour rejoindre **le Centre Collaborateur OMS France** sur les terminologies de Santé (2021) afin de **mieux diffuser les terminologies de l'OMS : CIM-10/11, ICHI, CIF, CISP, …**
- **Action 6 : Evaluation des terminologies de santé :** « Snomed-CT *versus* un panel de terminologies en usage » : publication des dernières annexes de l'étude (janvier 2021)
- **Action 7 : Entamer les négociations juridiques avec Snomed International** afin d'aplanir les **difficultés juridiques** et de permettre la mise à disposition d'une **version française traduite qualifiée**
- **Action 8 :** Réévaluer l'intérêt économique de la licence nationale de Snomed CT en **dénombrant le nombre de licence affiliées acquises en France**.

[29] https://www.phast.fr/blog/2020/03/31/phast-devoile-la-premiere-version-francaise-commune-de-snomed-ct/

❸ Gouvernance de l'interopérabilité des SI de Santé et du Médico-social

La mise en œuvre de la nouvelle gouvernance :

- **Publication** de la nouvelle gouvernance de l'interopérabilité dans le secteur santé social Janvier 2020 (après concertation).
- **1er comité de pilotage stratégique** avril 2020
- **1er comité de pilotage opérationnel** de l'interopérabilité septembre 2020

SYNTHESE DES ACTIONS CLES

Action	Jalons
CI-SIS : Production des volets génériques correspondants aux volets spécifiques déjà produits : accès à des connaissances externes, traçabilité,	Mise en concertation T1 2021
CI-SIS : Publication du MOS intégrant l'ensemble des concepts manipulés dans les cas d'usages génériques du CI-SIS	T1 2021
CI-SIS : Production des volets correspondant aux besoins d'interopérabilité identifiés lors du cycle de gouvernance 2020	2021-2022 en fonction des priorités attribuées à chacun
CI-SIS : Mise à jour du volet de contenu CDA	Fin 2019
CI-SIS : Produire des versions application mobile utilisant la norme FHIR pour les cas d'usage de partage de document et de gestion de dossier partagé	Publication version après concertation fin 2020
CI-SIS : outillage de test FHIR : prise en compte des volets non encore couverts (abonnement à notifications, accès à des recommandations externes et instanciation pour l'accès aux recommandations vaccinales…)	S1 2021
CI-SIS : Convergence des spécifications d'interopérabilité nationales des secteurs sanitaire, médico-social et social	Au fil de l'eau
CI-SIS : Mise à jour du formulaire de demande au CI-SIS mettant en exergue les exigences d'accompagnement du sponsor de la demande.	2021 T1
CI-SIS : Réflexion sur le Rôle des GRADeS dans le déploiement de l'interopérabilité et l'accompagnement terrain	2021 T1
CGTS : création du CGTS (2019), ouvertures des services d'accompagnement (2020)	2019- 2020
CI-SIS : Cartographie AFNOR des travaux de normalisation internationale en informatique de santé, priorisation avec les acteurs de l'écosystème (industriels…) des commissions, instances… de normalisation au niveau international (CEN, ISO) à suivre par la France	2021 T3
CGTS : Mise à disposition des terminologies. Catalogue (2019), ouverture du SMT (novembre 2020), puis deux versions du SMT en 2021	2019- 2020-2021

CGTS : Préparation technique (mise eu format pour publication) des terminologies : LOINC (jeux de valeurs LOINC et Circuit de la biologie) CISP2, ADICAP, Médicabase, Cladimed, (2019), CIM11, NABM	2019 2020 2021
CGTS : Evaluation de terminologies de santé : Snomed-CT versus un panel de terminologies en usage, (publication de l'étude fin 2020)	2020
L'ANS candidate pour rejoindre le Centre Collaborateur OMS France sur les terminologies de Santé (fin 2020)	2020 2021 2022
Gouvernance : nouvelle version des règles de gouvernance du CI-SIS	2021 T1

POUR EN SAVOIR PLUS

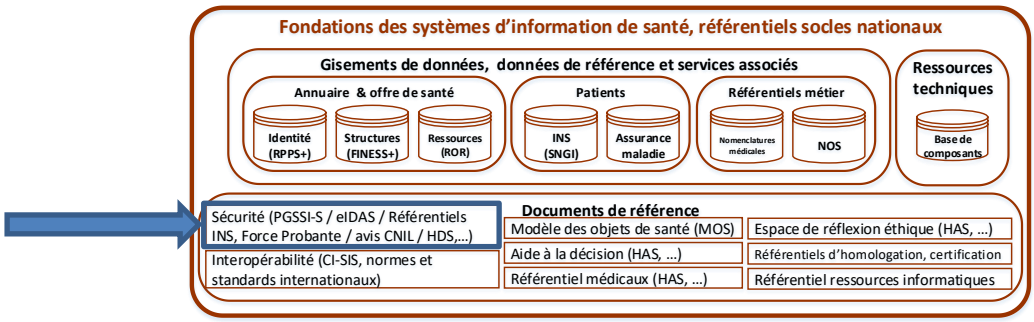
L'espace interopérabilité du site esante.gouv.fr (esante.gouv.fr/interopérabilité) permet d'accéder :

- Au contenu du cadre d'interopérabilité des systèmes d'information de santé,
- Au modèle et nomenclatures des objets de santé,
- Au catalogue des terminologies de santé et à une présentation du Centre de Gestion des Terminologies de Santé.
- Au serveur multi-terminologies https://smt.esante.gouv.fr/ ,
- A l'espace de tests d'interopérabilité https://esante.gouv.fr/interoperabilite/espace-de-tests-dinteroperabilite .
- Le CI-TLSi accessible sur le site site du GIE Sesam-Vitale : https://industriels.sesam-vitale.fr/

Le plan d'actions détaillé des travaux prévus en matière d'interopérabilité est publié dans esante.gouv.fr.

4 – Sécurité des systèmes d'information de santé

4.1. Politique générale de sécurité des systèmes d'information de santé (PGSSI-S)



DOCTRINE

L'Etat confie à l'ANS l'élaboration et la publication de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), **cadre à respecter** par tous les acteurs de la santé et du médico-social pour **sécuriser le système d'information de santé.** L'opposabilité de la PGSSI-S est assurée par l'enchainement documentaire PSSI-E (état), PSSI MCAS (Ministères sociaux) et PGSSI-S. **Il s'applique notamment :**

- Aux industriels dans leurs choix relatifs à la sécurité pour le développement de nouvelles offres ;
- Aux structures de santé dans la définition de leur politique de sécurité des systèmes d'information ;
- Aux porteurs de projet dans la définition des niveaux de sécurité à mettre en œuvre.

La PGSSI-S se compose de 2 types de documents :

- **Des référentiels, pour fixer et décrire les exigences de sécurité** des systèmes d'information portant sur :
  - L'identification électronique des acteurs des secteurs de la santé, du médico-social et du social,
  - L'identification électronique des patients et usagers du système de santé,
  - L'imputabilité (gestion de preuve et traçabilité),
  - La force probante des documents de santé ;
  - Le renforcement technique du niveau de sécurité.

- **Des guides de bonnes pratiques, pour accompagner les acteurs de santé,** décrivant les bonnes pratiques organisationnelles et techniques, à appliquer. Par exemple :
  - Guide d'élaboration et de mise en œuvre d'une politique de sécurité de système d'information,
  - Guide pratique spécifique à la destruction de données lors du transfert de matériels informatiques des Systèmes d'Information de Santé (SIS),
  - Guide des mécanismes de protection de l'intégrité des données stockées,
  - ….

Ces référentiels et guides de bonnes pratiques sont élaborés lors de groupes de travail avec des représentants de l'ensemble des parties prenantes, ils veillent à vérifier sa conformité au cadre de référence et réglementaire européen, puis sont mis en concertation publique.

La PGSSI-S se veut pragmatique et réaliste. A cet effet, les référentiels et les guides pratiques se présentent avec une notion de paliers : **un palier minimal et des paliers progressifs**, permettant aux porteurs de projet **d'améliorer progressivement la sécurité** de leurs projets jusqu'au palier cible défini selon leur contexte. Elle est régulièrement mise à jour pour s'adapter aux évolutions industrielles et technologiques, aux usages et aux évolutions réglementaires.

TRAJECTOIRE

Les premières publications de la PGSSI-S datent de 2013.
Portés par l'ANS, les **travaux d'évolution de la PGSSI-S et des modalités de sa mise en œuvre se déclinent sur 4 axes** :

Axe 1 : Mettre à jour et élaborer de nouveaux documents dans la PGSSI-S :

Référentiels :

- Publication d'un nouveau référentiel relatif à la **force probante des documents de santé** (T1 2021) ;
- Publication d'un nouveau référentiel **d'identification électronique des patients et usagers du système de santé** (T3 2021) ;
- Mise à jour des référentiels d'identification et d'authentification des acteurs de santé (T3 2021) pour y intégrer les évolutions liées à la feuille de route « accélérer le virage numérique » ainsi que le positionnement par rapport aux niveaux eIDAS ;
- Mise à jour du référentiel sur l'imputabilité (T3 2021).

Autres documents :

- Tout guide de bonnes pratiques ou document d'accompagnement pour lequel un besoin a été identifié dans le cadre de la gouvernance de la PGSSI-S (cf. axe 2).

Axe 2 : Renforcer la gouvernance autour de la PGSSI-S

Pour permettre cette mise-à-jour, de façon adaptée au développement rapide de l'usage du numérique en santé, l'Etat renforce la gouvernance de la PGSSI-S.

a. Collecte des besoins au plus près du terrain

- **Les besoins relatifs à la PGSSI-S sont collectés via :**
  - L'observatoire des incidents proposé par la cellule Accompagnement Cybersécurité des Structures de Santé (ACSS),
  - L'observatoire des vulnérabilités (service national de cybersurveillance tel que décrit dans l'action 9 de la feuille de route virage numérique),
  - L'observatoire de la conformité (action 8 de la même feuille de route),
  - Des échanges directs avec les acteurs du secteur (professionnels, structures, industriels, institutionnels…) ;

b. Formalisation des processus d'élaboration et de la gouvernance associée

- Les processus gouvernance sont définis afin de :
  - Valider l'opportunité de nouveaux référentiels ou guides de bonnes pratiques ou d'évolution des documents existants,
  - Composer des groupes de travail pertinents sur les thèmes abordés avec des représentants de l'ensemble des parties prenantes (professionnels, industriels, institutionnels…)
  - Encadrer la concertation publique sur chacun des référentiels et des guides de bonnes pratiques publiés.

- **L'objectif de ces processus est de s'assurer, d'une part, que la liberté de parole et l'équité sont respectées pour chacun des contributeurs et, d'autre part, que les échanges débouchent sur des livrables utiles au secteur.**

Axe 3 : Rendre opposables les référentiels et s'assurer de leur prise en compte au niveau des services numériques en santé financés sur fonds publics

Conformément à l'article L.1110-4-1 du code de la santé publique, les référentiels de sécurité élaborés par l'ANS peuvent être rendus opposables par arrêté du ministre de la santé. La mise en place de l'opposabilité fait l'objet d'une **étude.**

Les services numériques en santé financés sur fonds publics doivent être exemplaires en matière de sécurité. **Un dispositif de mesure de conformité aux référentiels de la PGSSI-S** est mis en œuvre pour ces systèmes (action 22 de la feuille de route virage numérique : CONVERGENCE).

Axe 4 : Accompagner les acteurs de santé et du médico-social

- Afin d'améliorer la prise en compte de la PGSSI-S, l'Etat propose un **accompagnement au changement adapté à chaque type d'acteurs.**
- Les modalités d'accompagnement varient en fonction des destinataires : **fiches réflexes synthétiques**, e-learning, tutoriels, tables rondes, webinaires, forums de discussion…

SYNTHESE DES ACTIONS CLES

Action		Jalon
Mettre à jour et élaborer de nouveaux documents de référence dans la PGSSI-S	Publication du référentiel relatif à la force probante des documents de santé	T1 2021
	Publication d'une nouvelle version du référentiel sur l'imputabilité	T3 2021
	Publication d'un nouveau référentiel d'identification électronique des patients et usagers du système de santé	T3 2021
	Mise à jour des référentiels d'identification et d'authentification des acteurs de santé pour y intégrer les évolutions liées à la feuille de route « accélérer le virage numérique » ainsi que le positionnement par rapport aux niveaux eIDAS	T3 2021
	Publication d'autres référentiels ou guides de bonnes pratiques	Au fil de l'eau en fonction des besoins
	Publication de la gouvernance formalisée	A définir

Renforcer la gouvernance autour de la PGSSI-S	Mise en œuvre des processus de gouvernance formalisé (collecte de besoins, validation de besoins, élaboration de documents, concertation publique)	Au fil de l'eau à partir de T3 2021
Rendre opposables les référentiels et s'assurer de leur prise en compte au niveau des services numériques en santé financés sur fonds publics	Etude des conditions pour rendre opposables les référentiels de la PGSSI-S	T4 2020
	Analyse et formalisation du processus pour rendre opposables les référentiels de la PGSSI-S	S1 2021
	Mise en œuvre du processus pour rendre opposables les référentiels de la PGSSI-S	Au fil de l'eau à partir de S1 2021
Accompagner les acteurs de santé et du médico-social	Identification des différents types d'acteurs à accompagner	S1 2020
	Définition des modalités d'accompagnement de chaque type d'acteur	T3 2020
	Elaboration des supports d'accompagnement pour chaque type d'acteur	Au fil de la publication de référentiels à partir de T1 2021
	Accompagnement des acteurs du secteur	Au fil de la publication de référentiels à partir de 2021

SYNTHESE DES IMPACTS POUR LES MOE ET MOA

Synthèse des impacts pour les MOA (Structures de santé, GRADeS…)

- Consultation des référentiels publiés à partir de T4 2020 et prise en compte des exigences : mise à jour de la politique de sécurité des systèmes d'information locale, adaptation de outils, des processus et procédures afin d'être en conformité avec la PGSSI-S.

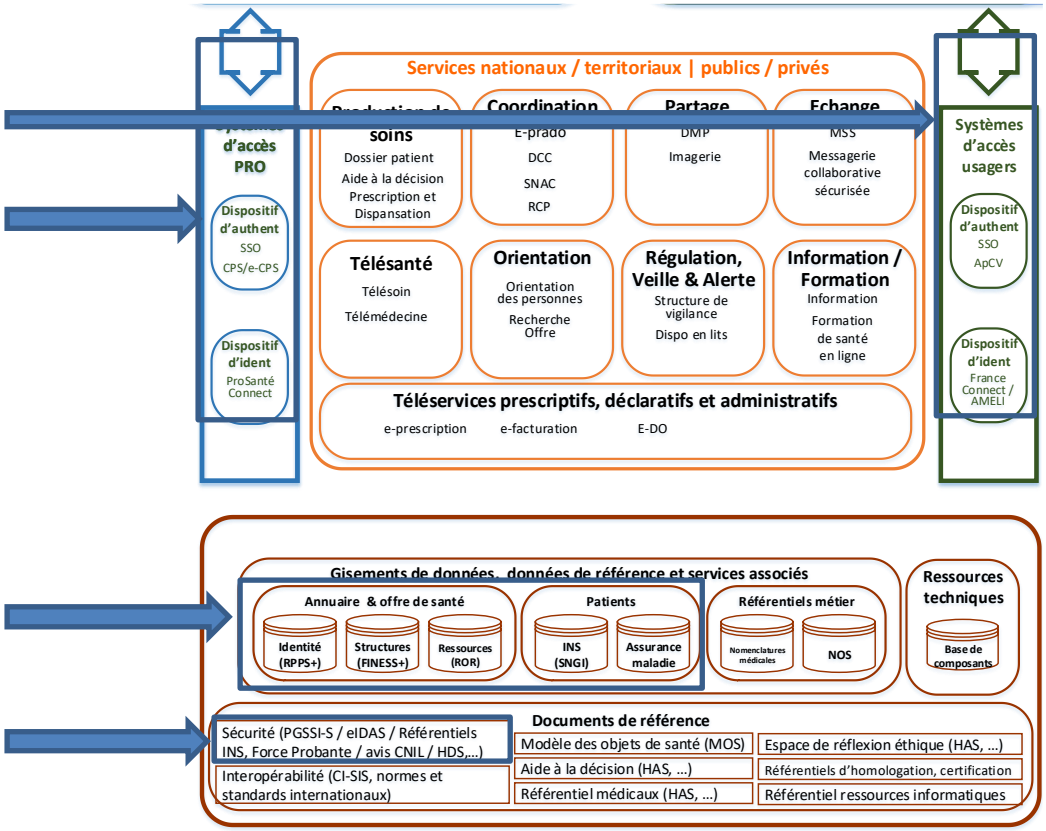
Synthèse des impacts pour les MOE (Industriels)

- Consultation des référentiels publiés à partir de T4 2020 et prise en compte des exigences : ajustements des solutions proposées afin de proposer aux structures de santé des outils et solutions conformes à la PGSSI-S.

POUR EN SAVOIR PLUS

https://esante.gouv.fr/securite/politique-generale-de-securite-des-systemes-d-information-de-sante

4.2. Identification électronique et répertoires de référence (INS, RPPS, FINESS)



L'identification électronique (IE) est, selon les définitions du règlement européen eIDAS[30], le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale. Au cœur de ce processus, qui regroupe à la fois les enjeux d'identification et d'authentification, figurent les questions suivantes :

- Comment enrôler/enregistrer une personne chez un fournisseur d'identité (FI) ?
- Quels types de moyens d'identification électroniques (MIE) lui donner une fois enrôlé (exemples : application mobile, certificats, mots de passe et secrets plus ou moins complexes, facteurs biométriques, facteurs dynamiques changeant à chaque authentification, etc.) et comment maintenir (expiration, blocage en cas de vol, renouvellement en cas de perte ou d'oubli, etc.) ces MIE ?
- Quelles données récupèreront les fournisseurs de service (FS) lors de l'IE d'une personne avec ces MIE ?
- Quels sont les répertoires d'identification de référence[31] et comment l'enrôlement y est fait ?
- Comment permettre à un FS de recoller aux données des répertoires de référence si le fournisseur d'identité n'a pas directement servi ces informations au FS ?

Les contrôles d'accès (CA) sont les autorisations/habilitations au sein du FS. Ça n'est pas parce que je sais avec un bon degré de confiance qui est derrière son écran / au bout du fil / devant moi que je veux forcément lui donner un accès. Comme les CA sont parfois déduits automatiquement d'attributs fournis lors de l'IE (profession, secteur d'activité, etc.), les deux notions (IE et CA) ont parfois été

[30] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/referentiel-documentaire-lie-au-reglement-eidas/

[31] INS - RNIPP/SNGI - pour les usagers, RPPS pour les acteurs de santé personnes physiques (ASPP), FINESS pour les acteurs de santé personnes morales (ASPM)

confondues, créant des difficultés. Il est néanmoins courant et recommandable d'avoir des CA paramétrés par des administrateurs locaux et/ou les personnes directement concernées par les données (patients, professionnels, etc.).

L'IE et les CA souffrent d'une maturité hétérogène dans le domaine de la santé avec :

- Certains professionnels privés d'usages numériques en l'absence d'enregistrement chez les FI de référence (RPPS notamment) et d'obtention de MIE associés (e-CPS notamment) ;
- Un niveau de sécurisation qui reste largement à améliorer dans de nombreux traitements, que ça soit au niveau d'un enrôlement peu fiable ou de facteurs d'authentification trop faibles ;
- De réelles difficultés pour de nombreux fournisseurs de services (FS) numériques en santé dans la gestion de ces enjeux.

Pourtant, une bonne gestion de l'IE et des CA est essentielle au développement du numérique, en étant à la fois :

- Un levier pour permettre et simplifier les usages (permettre d'accéder à des services, passer d'un service à l'autre sans rupture, etc.) ;
- Une garantie pour la sécurité, contre les risques d'usurpation, de fraude ou de vol de MIE ;
- Un pilier de l'interopérabilité, avec l'utilisation d'identifiants de portée nationale (RPPS, INS, FINESS) pour automatiser certains rattachements de données.

Afin d'apporter une réponse concrète à ces problématiques, l'Etat met à disposition la présente doctrine pour l'IE et les CA, donnant de la visibilité aux acteurs et définissant de façon macroscopique les grandes orientations et les niveaux de garantie exigés ainsi que les systèmes privilégiés ou exigés, tout en laissant aux différents traitements de la flexibilité sur les technologies et les FI qu'ils choisiront d'utiliser, ainsi que la possibilité d'aller plus loin dans la sécurité (niveau de garantie IE, CA en « opt-in », etc.) en fonction de l'analyse de risque effectuée par le ou les responsables de traitement.

Cette doctrine sera déclinée dans quatre chapitres de la PGSSI-S qui deviendront opposables en application de l'article L1110-4-1[32] du code de la santé publique (référentiels de sécurité et d'opposabilité) et des articles de loi créés par l'ordonnance identification électronique. Ces quatre chapitres sont :

- IE des usagers (personnes, citoyens, patients, aidants, etc.) et leur identité INS ;
- IE des acteurs de santé personnes physiques - ASPP (ex : médecins, secrétaires médicales, etc.) et leur identité RPPS ;
- IE des acteurs de santé personnes morales - ASPM (ex : centre hospitalier, CPTS, service numérique référencé dans le store de l'ENS, etc.) et leur identité FINESS/SIREN ;
- Gestion des contrôles d'accès.

Les objectifs poursuivis sont les suivants :

1. Assurer aux citoyens un niveau de garantie minimal et homogène dans l'accès à leurs données de santé et faire progressivement monter l'écosystème en maturité sur la sécurité de l'IE et des CA ;
2. Faciliter l'accès aux services numériques en santé pour les usagers et la navigation entre ces services ;
3. Décharger les fournisseurs de services (FS) de l'IE, au profit d'un nombre réduit de FI délivrant et maintenant des MIE ;
4. Promouvoir les répertoires de référence dans l'identification des acteurs (INS, RPPS, FINESS), piliers de l'interopérabilité.

[32] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036515027/

Des grandes orientations de doctrine transversales sur l'identification électronique

- Les FS arrêtent progressivement d'être leurs propres FI, tout en pouvant conserver un processus d'enrôlement et des accès propres pour des cas dérogatoires. **Les FI sont factorisés** en un nombre limité d'acteurs dont c'est le métier. Cela permet aux FS de se concentrer sur leurs services à valeur ajoutée, de se décharger des complexités associées à l'identification électronique et de renforcer le niveau de sécurité en mutualisant les FI. Ces derniers sont :

    - Complémentaires et parfois concurrentiels en ce qui concerne les usagers – avec un fournisseur d'identité de référence : l'Assurance Maladie avec l'ApCV ;

    - Largement fournis par l'état en ce qui concerne les professionnels enregistrés au RPPS au travers du fournisseur d'identité de référence : l'Agence du Numérique en Santé avec les CPS, les applications mobiles e-CPS et, plus globalement, les certificats de l'autorité de certification IGC-Santé.

- Les FI peuvent être regroupés dans des fédérateurs accessibles aux FS satisfaisant à certains critères (finalités, etc.), généralement basés sur le protocole standard Open ID Connect[33] : France Connect pour les usagers et Pro Santé Connect pour les ASPP. Les FS peuvent utiliser plusieurs types de clients et solutions de gestion des identités et des accès. Les FS peuvent permettre aux usagers de déconnecter leur session du fédérateur. Les fédérateurs peuvent proposer des mécanismes complémentaires de type « fournisseur de données » ;

- Le règlement eIDAS définit 3 niveaux de garantie (I – faible, II- substantiel, III- fort). En fonction de la sensibilité des données dont ils ont la charge, un niveau de garantie minimal est exigé aux FS, avec une cible ambitieuse à 5 ans sur l'usage exclusif de FI de niveau substantiels eIDAS pour l'IE des usagers. Un niveau intermédiaire, entre faible et substantiel, dit « renforcé », est défini plus loin dans cette doctrine. Ce palier temporaire et intermédiaire, visant à une montée progressive du niveau de sécurité de l'identification électronique, n'a pas de portée au-delà du secteur de la santé en France ;

- Il est essentiel de référencer les données avec les identifiants de référence (INS, RPPS, FINESS/SIRET) pour permettre leur interopérabilité ultérieure. Ces informations peuvent être directement « servies » par le fournisseur d'identité ou le fédérateur, ou encore par des requêtes sur les couches d'exposition des répertoires sectoriels de référence (téléservice INSi, exposition RPPS/RASS en REST/FHIR, exposition FINESS) ou à minima par l'utilisation de fichiers complets mis à jour régulièrement ;

- Il est important d'accompagner les utilisateurs dans ces évolutions, par la mise en place d'un centre de support et d'accompagnement des acteurs sur l'identification électronique et les contrôles d'accès.

[33] https://openid.net/connect/

4.2.1. Identité électronique des usagers

Les services numériques de santé concernés par ce présent cadre de référence sont les **services traitant des données de santé à caractère personnel, au sens du RGPD**[34].

DOCTRINE

4.2.1.1. Niveau de garantie cible des fournisseurs d'identité intégrés par les fournisseurs de services

Au 1er janvier 2023 (dans 2 ans), il est attendu, pour ces services numériques qu'ils implémentent exclusivement des FI/fédérateurs certifiés eIDAS substantiel ou ayant un niveau de garantie «renforcé », tel que défini ci-après.

À cette échéance**,** il est attendu, pour ces services numériques ne disposant pas encore de FI certifiés substantiels eIDAS, que leurs FI (éventuellement eux-mêmes) atteignent un niveau de garantie équivalent eIDAS renforcé, défini ci-après. Cela correspond à des solutions d'identification électroniques impliquant :

- **Un enrôlement basé sur une vérification de l'identité de la personne la plus fiable possible**, avec :
  - Une dérivation de l'identité France Connect – si possible de niveau substantielle ; et/ou
  - La vérification d'une pièce d'identité à haut niveau de garantie, éventuellement dématérialisée (scan), si possible confrontée à l'utilisateur (photo, vidéo ou face à face) ; et
  - Dans le cas d'utilisation de l'adresse électronique et/ou du téléphone mobile comme moyen d'identification électronique ou dans le processus de récupération du moyen d'identification électronique, une vérification de ces coordonnées par l'envoi d'un code ou d'un lien d'activation.
- **Des moyens d'identification électroniques basés** :
  - Soit sur un unique couple login / mot de passe, en respectant alors strictement les critères associés au Cas n°2 - *Mot de passe et restriction d'accès au compte*, ou au Cas n°3 - *Mot de passe et information complémentaire* ou au Cas n°4 - *Mot de passe et matériel détenu par la personne* de la délibération CNIL n° 2017-012 du 19 janvier 2017 (le Cas n°1 – Mot de passe seul est exclu). À toutes fins utiles, les critères du cas le moins restrictif (Cas n° 2) sont rappelés ci-après :
    - La taille du mot de passe doit être au minimum de 8 caractères ; et
    - Le mot de passe doit au minimum comporter 3 des 4 catégories de caractères (majuscules, minuscules, chiffres et caractères spéciaux) ; et
    - L'authentification doit faire intervenir une restriction de l'accès au compte, qui doit prendre une ou plusieurs des formes suivantes :
      - Une temporisation d'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement dans le temps ; la commission

[34] https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

recommande que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives par 24 heures ; et/ou

- Un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (p. ex. : « captcha ») ; et/ou
- Un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10.

- Soit sur une authentification à deux facteurs de différentes catégories (possession, connaissance, attributs de la personne). Ces deux facteurs peuvent n'être exigés qu'à la première identification électronique et, à échéance régulière ou au changement de type de connexion (navigateur, IP, adresse mac, etc.). L'utilisation d'un facteur d'authentification dynamique est recommandée.

Exemple : dans le cas d'un service fourni sur une application mobile, cela peut par exemple constituer en l'utilisation d'une clé (1er facteur) contenue dans l'application enrôlée, accessible par empreinte digitale / faciale non envoyée au fournisseur de services, et l'utilisation nécessaire, à échéance régulière, d'un code temporaire accessible par une application spécialisée (ex : Authentificator, Authy, VIP Access, etc.).

Dans tous les cas, il est fortement recommandé d'envoyer par défaut par e-mail, à chaque identification électronique ou à échéance régulière, un récapitulatif des identifications électroniques (avec date et heure, nom de l'appareil, navigateur, etc.), et de référencer la liste des identifications électronique dans un onglet de l'éventuel compte de l'utilisateur, en lui permettant de signaler au responsable de traitement d'éventuels doutes sur des accès frauduleux à son compte.

Au 1er janvier 2026 (dans 5 ans), il est attendu, pour ces services numériques qu'ils implémentent **exclusivement** des FI/fédérateurs certifiés eIDAS substantiel.

Cet objectif est placé à moyen terme du fait de la faiblesse de l'offre actuelle en fournisseurs d'identité avec ce niveau de garantie et le temps que prendra un enrôlement de suffisamment de citoyens chez ces fournisseurs d'identité.

Il respecte un principe de libre concurrence : aucun FI / MIE n'est imposé, et cela permet de laisser le choix au patient entre les FI dans lesquels il a le plus confiance et les MIE qui correspondent le mieux à ses usages.

L'ApCV est néanmoins le futur FI de référence qui est recommandé pour les FS du domaine de la santé.

France Connect est un fédérateur de FI recommandé, ouvert aux FS privés (expérimentation en cours, notamment dans le domaine de la santé) et publics, qui permettra de restreindre l'accès aux FI de niveau substantiel eIDAS. Il s'intègre facilement pour les FS et permet au patient de naviguer entre les FS sans ré-identification électronique visible par l'utilisateur.

4.2.1.2. L'identité nationale de santé (INS), provenant des répertoires RNIPP/SNGI

La loi[35] consacre **le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) comme matricule identifiant national de santé (INS) des personnes pour leur prise en charge à des fins sanitaires et médico-sociales**. Le matricule INS est soit le NIR pour les personnes immatriculées, soit le NIA (numéro identifiant d'attente) pour les personnes en attente d'immatriculation. Des solutions alternatives seront proposées dans les versions ultérieures de cette doctrine pour les personnes n'en disposant pas (numéro national provisoire - NNP - pour les bénéficiaires de l'AME, etc.).

Depuis le 1er janvier 2021, le référencement des données de santé avec l'identité INS est obligatoire pour les acteurs de la prise en charge.

L'Etat fournit à ces acteurs un accès aux données de l'identité INS (Matricule INS complété par un OID[36], et cinq traits : nom de naissance, prénom(s) de naissance, sexe, date de naissance, lieu de naissance) issues des bases de référence (répertoires RNIPP/SNGI) par la mise à disposition du téléservice (INSi). Le téléservice INSi propose deux familles d'opérations : l'une permettant de récupérer une identité INS (opération de récupération) et l'autre permettant de vérifier une identité INS (opération de vérification), accessibles pour les acteurs de santé.
Un arrêté rend opposable le « référentiel INS » qui décrit les exigences associées au référencement des données de santé avec l'identité INS, qui s'appliquent aux responsables du référencement des données ainsi qu'à leurs éventuels sous-traitants (éditeurs, etc.).

Par ailleurs, un référentiel national d'identitovigilance (RNIV) a été construit en 2020 avec le réseau des référents régionaux d'identitovigilance (3RIV) et mis à concertation. Il sera rendu opposable début 2021. Il distingue une identité :

- **Validée**, lorsqu'elle a fait l'objet d'une identification électronique de niveau eIDAS substantiel ou d'une vérification d'un titre d'identité à haut niveau de confiance ;
- **Récupérée**, lorsqu'elle a été récupérée ou vérifiée par l'intermédiaire du téléservice INSi, ou d'un dispositif équivalent (application carte vitale – ApCV) ;
- **Qualifiée**, lorsqu'elle est à la fois **validée** et **récupérée**. Ce statut permet, lors de l'échange ou du partage d'une donnée de santé, d'y associer l'identité INS (selon des formats définis dans une annexe du CI-SIS) afin que le destinataire puisse automatiquement associer la donnée de santé au bon patient lors de la réception.

Une identité n'ayant été ni validée, ni récupérée est considérée comme une identité provisoire. Ce statut ne permet pas, lors de l'échange ou du partage d'une donnée de santé, d'y associer l'identité INS.

Pour mettre en œuvre l'identité INS, les éditeurs doivent être en capacité :

- D'interroger le téléservice INSi pour récupérer et/ou vérifier l'identité INS, en se basant sur le guide d'intégration du GIE SESAM-Vitale. Le respect du guide d'intégration est validé par une autorisation octroyée par le centre national de dépôt et d'agrément (CNDA[37]) ; et/ou
- De gérer les identités, et en particulier les identités INS, conformément au référentiel INS et aux bonnes pratiques d'identitovigilance décrites dans le RNIV, en se basant sur le guide

[35] Article L. 1111-8-1 du code de la santé publique

[36] OID : Object Identifier correspondant à l'identifiant de la structure à l'origine de l'attribution du NIR ou du NIA. Le NIR et le NIA ont chacun leur organisme d'affectation. L'OID permet de les distinguer.

[37] https://cnda.ameli.fr/

d'implémentation de l'identité INS de l'ANS. Ce guide d'implémentation sera rendu opposable au T1 2021 en annexe du référentiel INS ;
- De diffuser l'identité INS dans les flux et les fichiers conformément aux standards d'interopérabilité en vigueur, en se basant sur l'annexe INS du CI-SIS (qui référence également les standards maintenus par InteropSanté).

À terme, l'ApCV permettra de qualifier directement l'identité car (i) elle sera un FI certifié eIDAS substantiel et (ii) elle servira l'identité INS provenant d'un appel au téléservice INSi réalisé par l'ApCV. Un fournisseur de services implémentant l'ApCV hors France Connect pourra donc récupérer directement qualifier l'INS du patient et se dispenser d'un appel au téléservice INSi.

Lors d'une IE par France Connect, les traits de l'identité pivot sont redressés par France Connect au RNIPP : c'est-à-dire dont l'identité a été éventuellement remplacée par une identité très proche au RNIPP. Ceci est valable au moins pour les fournisseurs d'identité de niveau faible, des discussions sont en cours pour s'assurer qu'une identité redressée RNIPP – complémentaire et non remplacée – sera également transmise dans le cas pour les fournisseurs d'identité de niveau substantiel et élevé. Ces traits peuvent faire l'objet d'une requête à INSi par le FS pour récupérer l'identité INS. Un mécanisme intermédiaire entre « Fourniture de l'identité INS avec le matricule dans l'identité pivot » et « France Connect - Fournisseur de données » pourrait, à terme, voir le jour, pour fournir directement l'identité INS aux fournisseurs de services acteurs de la prise en charge, en complément d'INSi et de l'ApCV.

4.2.1.3. Zoom sur les serveurs régionaux d'identité, les serveurs régionaux de rapprochement des identités et l'INS

La cible

L'identité INS devient le pivot des échanges de données entre les acteurs de santé. L'ensemble de ces acteurs respectent le référentiel INS et le référentiel national d'identitovigilance (RNIV). Concernant les cas résiduels sans INS, la doctrine sera précisée ultérieurement.

L'éventuelle fonction de "rapprochement" (SRRI) des SRI disparait.

L'éventuelle fonction de "GAM régionale" (SRI) / "référentiels d'identité commun aux services régionaux" des SRI peut perdurer. En effet, 2 options d'urbanisation sont possibles pour les régions :

- **Option 1 :** Chaque service régional dispose d'une base d'identités qui lui est propre ;
- **Option 2 :** Les services régionaux s'appuient sur une "GAM régionale".

Dans les deux cas, il est obligatoire d'y référencer l'identité INS dans les conditions prévues par le référentiel INS, le référentiel national d'identitovigilance, le guide d'implémentation de l'INS et le guide d'intégration du téléservice INSi.

Dans la configuration "Option 2" il convient d'être vigilant aux points suivants :

- Un fonctionnement des services régionaux sans la GAM régionale doit être possible de manière à faciliter leur mutualisation et leur intégration au futur bouquet de services (BSP), en partie grâce à la gestion de l'identité INS ;
- La qualification de l'identité INS doit être effectuée dès que possible lors de la prise en charge d'un patient/usager par l'intermédiaire des acteurs de la prise en charge, dans l'un des services régionaux grâce au téléservice INSi ;

- L'identité INS ne doit être accessible qu'aux acteurs de l'équipe de soins, responsables de la prise en charge. A ce titre, chaque organisation utilisant un service régional devra garantir la sécurité de l'identité INS au même titre qu'une donnée de santé, avec le cloisonnement nécessaire ;
- S'il doit demeurer un identifiant technique régional au sein de la GAM régionale, il n'est en aucun cas transmis en externe du SI régional (aux établissements, etc.) dès lors que l'identité est qualifiée (seule l'identité INS est transmise). Il peut être transmis uniquement lorsque l'identité n'est pas qualifiée et s'il est nécessaire de fournir un identifiant de par les contraintes d'interopérabilité des messages transmis. Autrement, seuls les traits d'identité, récupérés au téléservice INSi ou non, sont transmis. De la même manière, aucun établissement du territoire n'utilise l'identifiant technique régional dans ses échanges : ils utilisent exclusivement l'identité INS lorsqu'elle est qualifiée et, à défaut, l'IPP local de la structure.

Plus globalement, lorsque l'identité INS est qualifiée par un acteur, le matricule INS est le seul identifiant partagé par cet acteur.

Les services régionaux ne peuvent pas être une modalité de distribution de l'identité INS aux acteurs de la région, qui doivent recourir au téléservice INSi. En revanche les outils régionaux partagent des données de santé "en aval" avec l'identité INS, comme tout outil de prise en charge des données de santé.

Pour les transferts d'informations de santé entre des acteurs et les services régionaux (ou tout autre acteur), l'identité n'est transmise que lorsqu'il y a une prise en charge prévue chez l'acteur en aval. Cela peut prendre la forme d'une demande ou prescription électronique mais ne doit pas faire l'objet d'une transmission systématique (hors prise en charge de l'usager).

Les prérequis et la temporalité de l'atteinte de cette cible

La cible doit être atteinte fin 2022, sous réserve que :

- 90% des données de santé soient effectivement partagées avec l'identité INS (mesurée dans les documents du DMP et/ou dans les échanges par MSS) ;
- Les solutions régionales puissent récupérer l'identité INS au téléservice INSi grâce à une identification électronique des personnes morales (évolution envisagée pour Avril 2021).

Les acteurs au niveau national (ANS, GIE SESAM-Vitale) et dans les territoires (ARS, CPAM (CIS), GRADeS, URPS, etc.) mettent en œuvre des actions de communication, d'incitation et d'accompagnement des acteurs.

Des indicateurs et des cibles sont construits par le projet INS (équipe DNS-ANS-Cnam) et les régions pour suivre l'avancée du déploiement de l'INS. Ils émanent du téléservice INSi, du GIE SESAM-Vitale, des éditeurs et des acteurs territoriaux. Ils sont régulièrement révisés.

La phase transitoire (durée prévisionnelle : 2 ans, jusqu'à fin 2022)

Concernant l'utilisation de l'éventuelle fonction de "GAM régionale" (SRI) / "référentiels d'identité commun aux services régionaux" un dispositif temporaire n'est pas nécessaire.

Concernant l'utilisation de l'éventuelle fonction de "rapprochement" (SRRI) des serveurs régionaux d'identité, un dispositif temporaire peut être nécessaire pour assurer la continuité des usages actuels et permettre de contribuer au déploiement de l'identité INS, dans le respect des mesures du référentiel national d'identitovigilance.

Dans la phase transitoire, l'identité INS peut être référencée dans les serveurs de rapprochement.

À partir de la possibilité d'identification électronique au téléservice INSi pour les personnes morales, les structures (GHT, etc.) non encore connectés à des SRRI ne devront plus s'y raccorder, afin de se focaliser sur l'intégration d'INSi et l'implémentation de l'identité INS au sein de leurs structures.
Entre-temps ou en cas d'impossibilité avérée à se connecter au téléservice INSi, cette connexion est possible, mais le déploiement de l'identité INS par l'appel au téléservice INSi doit être prioritaire sur le déploiement des serveurs régionaux de rapprochement d'identités.

Pour les structures qui y sont déjà connectées et dans le cadre d'échanges de données de santé, les serveurs de rapprochement peuvent continuer à être utilisés en période transitoire en s'assurant qu'ils n'instaurent pas une situation de dépendance durable des acteurs à ces derniers, au détriment de l'implémentation de l'identité INS.

Par exemple, lors de la réception d'une donnée de santé, le SRRI peut transitoirement permettre au destinataire des données, lors de la réception d'une donnée de santé :

- S'il n'a pas implémenté l'INS mais que c'est le cas de l'expéditeur, de récupérer auprès du SRRI son identité locale à partir de l'identité INS reçue de l'expéditeur ;
- S'il a implémenté l'INS, de récupérer auprès du SRRI l'identité INS à partir de l'identité locale de l'expéditeur dans le cas où ce dernier n'implémente pas l'INS. Cela permet au destinataire de classer directement la donnée de santé dans le bon dossier. Attention, cet usage n'est possible que si l'identité INS est déjà qualifiée chez le destinataire. Si ça n'est pas le cas, l'identité INS fournie par le SRRI ne peut pas servir, comme INSi, à "qualifier" l'identité INS chez le destinataire.

En période transitoire et en l'attente de flux informatisés de "prescription de prise en charge", la mise à disposition proactive et systématique d'identités des acteurs aux services régionaux ne peut se faire que dans un encadrement contractuel strict et d'un respect du RGPD et du principe de minimisation des données.

4.2.1.4. Zoom sur l'identité INS dans les GHT

Dans la ligne des exigences réglementaires (article L6132-3 et R6132-15 du code de la santé publique), les SI de GHT doivent faire l'objet d'une convergence et utiliser un référentiel d'identité unique. Ce dernier peut être construit autour du matricule INS ou d'un autre identifiant local coexistant avec l'identité INS. Cette dernière doit être implémentée au plus vite dans l'ensemble du SI des établissements (GAM, EAI, DPI, SGL, RIS, PACS, etc.).

En cible, il est nécessaire que les ES de GHT puissent converger vers une gouvernance et des processus (formation, suivi, gestion des cas complexes, etc.) transversaux sur l'identitovigilance, ainsi que vers une GAM multi-entités. L'atteinte de ces objectifs permet la réutilisation des travaux de qualification de l'INS effectués par un autre établissement.

En transitoire :

- L'INS doit être implémenté dans chaque référentiel d'identité de chaque établissement, notamment dans la perspective d'un partage de données de santé intra-GHT et avec l'extérieur ;
- Si certains utilisent des serveurs de rapprochement (instance GHT), l'identité INS qualifiée par un établissement peut être diffusée par ce biais à un autre établissement à l'occasion d'une prise en charge sous réserve que la GAM du destinataire puisse permettre l'implémentation de l'INS et que le rapprochement / la recherche d'antériorité se fasse exclusivement sur les cinq traits de l'identité INS : nom de naissance, liste des prénoms, date de naissance, sexe et lieu de naissance. Le destinataire doit procéder à la qualification de l'identité INS dans sa GAM,

sauf à avoir contractualisé avec l'établissement expéditeur dans les conditions dérogatoires définies dans le référentiel national d'identitovigilance pour les sous-traitants.

4.2.1.5. Zoom sur des acteurs spécifiques référençant l'INS et le NIR

Certains acteurs n'appartenant pas au cercle de confiance peuvent utiliser l'identité INS grâce à un texte spécifique encadrant l'utilisation de leur système d'information. Sont ainsi concernés, la Cnam, responsable de traitement du Dossier Médical Partagé[38] et du futur Espace Numérique de Santé ainsi que le Conseil National de l'Ordre des Pharmaciens (CNOP), responsable de traitement du Dossier Pharmaceutique (DP)[39].

Les traitements ayant pour finalité la prise en charge sont couverts par la réglementation relative à l'INS. Si un autre traitement de l'INS est mis en œuvre (hors finalité de prise en charge, hors acteur de la prise en charge), l'INS retombe alors dans la réglementation relative au NIR, il convient alors de respecter la loi informatique et liberté et notamment l'article 22 et le décret cadre NIR. La réutilisation de l'INS à des fins de recherche est couverte par le chapitre IX de la loi informatique et libertés.

4.2.1.6. Zoom sur l'ENS en tant que fournisseur de service

Pour les phases pilotes et généralisation en S2 2021, l'ENS sera son « propre FI » en ayant pris soin de reprendre les comptes existants pour le DMP (9,7 millions de DMP).

Il intégrera France Connect à partir du 1er janvier 2022, et verra en 2022 l'arrivée de l'ApCV comme FI complémentaire.

Il intégrera exclusivement, au plus tard à compter du 1er janvier 2026, dans le respect des exigences de la présente doctrine :

- Une IE par ApCV, entretemps certifiée substantiel eIDAS ;
- Une IE par France Connect, restreinte aux FI de niveau substantiel (ApCV, CNIé, La Poste, etc.).

Par ailleurs, au sein de l'ENS :

- Le matricule INS est l'identifiant de l'ENS, même s'il ne sera pas strictement obligatoire pour l'alimentation et qu'un mécanisme alternatif permettra de tenter de retrouver le matricule INS en cas d'absence d'identité qualifiée chez l'expéditeur des données ou si ce dernier n'est pas habilité à référencer l'identité INS ;
- Les contrôles d'accès (CA) seront, au moins en partie, directement gérés par le patient, avec, en ce qui concerne les accès des services référencés dans le store de l'ENS, des limites associés aux finalités des services référencés.

SYNTHESE DES ACTIONS CLES

Action	Jalon
Obligation de référencer les données de santé avec l'identité INS	1er janvier 2021
Nouvelle version du référentiel INS prévoyant l'identification électronique des personnes morales pour le téléservice INSi et	T1 2021

[38] Article R. 1111-33 du CSP dans sa rédaction issue du décret n°2016-914 du 4 juillet 2016 relatif au dossier médical partagé

[39] Article R.1111-20 du CSP dans sa rédaction issue du Décret n°2017-878 du 9 mai 2017 - art. 1

annexant le référentiel national d'identitovigilance et le guide d'implémentation INS	
Début de généralisation de l'ApCV (2 départements)	Avril 2021
Publication arrêté « référentiel identification électronique des usagers », après concertation	T4 2021
Lancement de l'espace numérique de santé (ENS)	1er janvier 2022
Poursuite de la généralisation de l'ApCV (12 départements)	Janvier 2022
Labellisation eIDAS substantiel de l'ApCV et démarrage de la généralisation France entière	Fin 2022
Cible d'usage de l'identité INS dans 90% des échanges de documents de santé	Décembre 2022
Atteinte d'un niveau minimum de garantie « renforcé » pour l'IE des usagers	1er janvier 2023
Atteinte d'un niveau de garantie eIDAS « substantiel » pour l'IE des usagers	1er janvier 2026

SYNTHESE DES IMPACTS POUR LES MOE ET MOA

Synthèse des impacts pour les MOA (Structures de santé, GRADeS…)

- Demander à ses éditeurs de faire évoluer les solutions d'IE des usagers ou de se doter de nouvelles solutions compatibles avec les exigences de 2023 et de 2026
- Demander à ses éditeurs d'intégrer le téléservice INSi
- Lancer un projet organisationnel sur les pratiques d'enregistrement et d'identitovigilance

Synthèse des impacts pour les MOE (Industriels)

- Intégration de nouveaux FI (ApCV, etc.), notamment au travers du fédérateur France Connect
- Obtention d'une autorisation CNDA pour INSi et modifications importantes de la gestion de l'identité dans le contexte de l'INS

POUR EN SAVOIR PLUS

https://franceconnect.gouv.fr/partenaires?source=homepage_header
https://esante.gouv.fr/securite/identifiant-national-de-sante
https://www.sesam-vitale.fr/web/sesam-vitale/insi2
https://solidarites-sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance
https://www.sesam-vitale.fr/appli-carte-vitale
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1502&from=FR
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033928007
https://blog.octo.com/wp-content/uploads/2020/11/authentification-717x1024.png

4.2.2. Identité électronique des Acteurs de Santé Personnes Physiques (ASPP)

Les services numériques de santé concernés par ce présent cadre de référence sont les **service, dits « prioritaires », définis comme traitant des données de santé à caractère personnel, au sens du RGPD**[40] et, pour se concentrer sur les traitements les plus importants, qui comportent au moins une des caractéristiques suivantes :

- Des services « partagés » définis comme dépassant le cadre d'une personne morale (ex : dépassant un GHT) et/ou à dimension nationale ou territoriale ;
- Des services intégrant fortement des services « partagés » (ex : dossier patient informatisé, etc.) ;
- Des services proposant un accès web externes aux SI, pour les professionnels d'un établissement ou leurs correspondants de ville ;
- Des services dont les traitements sont à grande échelle, notamment si le nombre de patients dont les données y sont référencées dépasse 50 000.

Pour les autres traitements référençant des données de santé, le niveau de garantie ci-après constitue uniquement une recommandation, mais il pourrait leur être élargi comme exigence dans des versions futures de la doctrine.

DOCTRINE

4.2.2.1. Niveau de garantie cible des fournisseurs d'identité intégrés par les fournisseurs de service

Au 1er janvier 2023 (dans 2 ans), il est attendu, pour ces services numériques qu'ils implémentent pour l'IE des ASPP : **(i) Pro Santé Connect** ET, s'ils le souhaitent (ii) des FI/fédérateurs certifiés eIDAS substantiel ou ayant un niveau de garantie «renforcé », tel que défini dans le chapitre sur les usagers, avec, en complément une vérification, à l'enrôlement, ainsi que de manière régulière et/ou lors de l'identification électronique, de l'existence de la personne dans les répertoires de référence (RPPS et, jusqu'à 2022, ADELI).

L'implémentation de Pro Santé Connect permet aux ASPP qui utilisent des services partagés de passer d'un service à l'autre sans apparente ré-identification électronique, d'éviter des ré-enrôlement systématiques dans les services partagés, et de permettre aux fournisseurs de services de se reposer, non forcément exclusivement, sur la puissance publique pour l'identification électronique de leurs usagers ASPP.

Indépendamment de la factorisation « nationale » avec Pro Santé Connect, il est fortement recommandé aux établissements de santé et médico-sociaux, ainsi qu'à leurs groupements (GHT, etc.), de factoriser leurs éventuelles modalités locales d'identification électronique, en se dotant de solution de type sigle sign-on (SSO) / identity and access management (IAM), afin d'harmoniser l'identification électronique entre applications locales.

Cela permet, entre autres :

- De monter le niveau de garantie de l'identification en une seule fois sur de multiples services ;

[40] https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

- De réduire le nombre de moyens d'identification électroniques pour les utilisateurs, ainsi que les processus d'enrôlement associés à leur délivrance ;
- De passer d'une application à l'autre ;
- D'organiser plus simplement des audits de l'identification électronique.

Au 1er janvier 2026 (dans 5 ans), il est attendu, pour ces services numériques qu'ils implémentent pour l'IE des ASPP : **(i) Pro Santé Connect** ET, s'ils le souhaitent (ii) des FI/fédérateurs certifiés eIDAS substantiel ou ayant une certification « sécurité de premier niveau (CSPN) dont le cahier des charges (*target of evaluation)* sera défini par l'ANS dans la continuité des critères du niveau « renforcé » évoqué dans le présent document.

Zoom : les MIE CPS et e-CPS (uniquement accessible par PSC) sont fournis par le fournisseur d'identité ANS. L'enregistrement au RPPS ne respecte pas actuellement les critères 'eIDAS substantiel' du fait de la variabilité des autorités d'enregistrement et de l'enjeu de les élargir pour inclure progressivement tous les professionnels intervenant en santé qui en ont besoin. Néanmoins :

- une certification des données au RNIPP est réalisée 1 fois par an ;

- des travaux sont en cours pour augmenter le niveau de garantie de l'enrôlement (et des ré-enrôlements / modifications de données) au niveau des différentes autorités d'enregistrement, en permettant de qualifier ce niveau au sein même du RPPS, permettant éventuellement aux fournisseurs de service d'accéder à cette information en fonction de leurs besoins.

4.2.2.2. Le répertoire de référence RPPS

À l'occasion de l'identification électronique, les FS ont l'obligation de référencer l'identifiant de portée nationale (RPPS, ADELI toléré jusqu'à fin 2022) ou, dérogatoirement, un identifiant de portée locale pour les traitements locaux isolés.

L'identité sectorielle doit être servie par le FI / MIE ou retrouvée immédiatement auprès des répertoires de référence après l'identification électronique grâce à un appariement sur les traits d'identités du professionnel ainsi recueillis. Grâce à cet identifiant, le FS peut aller chercher des données complémentaires (type de professionnel, code postal d'exercice, situation d'exercice, etc.) sur des couches d'exposition si elles ne sont pas fournies nativement par le FI / MIE.

Le RPPS a vocation à s'élargir d'environ 0,6M professionnels (6 professions à ordre : médecin, chirurgien-dentiste, sage-femme, pharmacien, masseur-kinésithérapeute, et pédicure-podologue) à environ 2M de professionnels intervenant en santé, avec notamment :

- L'enregistrement des infirmiers par l'ordre national infirmier (ONI) dès septembre 2021 : les infirmiers ne seront plus enregistrés dans ADELI et il est essentiels que les infirmiers salariés non-inscrits à l'ordre y procèdent (inscription obligatoire pour l'exercice de la profession) ;
- L'enregistrement des professions « périmètre ARS » (hors infirmiers) en trois vagues, dès juin 2021 (projet EPARS : les ARS enregistrent dans le RPPS avec l'outil ENREG où le professionnel peut demander son enregistrement et pré-remplir un certain nombre de données) ;
- L'enregistrement de nouvelles professions notamment à rôle des secteurs sanitaire et médico-social (aide-soignant, secrétaire médicale, etc.), par de nouvelles autorités d'enregistrement (employeurs, ARS, etc.), sur la base du même portail d'enregistrement (ENREG).

Une étude sera lancée en 2021 sur la pertinence de la création d'un service à compétence national, chargé, de l'enrôlement des professionnels (hors périmètre ordres) et de la qualité des données de référence les concernant.

Les professionnels peuvent se connecter à des espaces numériques de leurs autorités d'enregistrement (ex : pharmaciens, les infirmiers et les médecins ou un portail en absence de portail à l'autorité d'enregistrement) pour adapter certaines données de contact. L'identification électronique devrait, à terme, s'y faire par le fédérateur Pro Santé Connect et respecter les exigences de la présente doctrine en termes de niveau de garantie.

Le RPPS est la base de la délivrance des moyens d'identification électronique (MIE) carte CPS et application mobile e-CPS (voir ci-dessous).

Par ailleurs, les données publiques du RPPS sont accessibles via une interface homme-machine (l'annuaire santé : https://annuaire.sante.fr/), par la fourniture d'extractions sur le site de l'ANS et au travers de couches d'exposition en REST utilisant une modélisation FHIR des données. Il est conseillé aux fournisseurs d'identité et de services d'y avoir recours dès que de besoin, et notamment lors de l'identification électronique et à échéance régulière.

Le modèle des données du RPPS respecte le MOS-NOS : https://esante.gouv.fr/interoperabilite/mos-nos

4.2.2.3. Le moyen d'identification électronique « carte CPS »

La CPS est une carte délivrée régulièrement au domicile du professionnel lorsque celui-ci en a besoin. Elle dispose d'un code PIN. Les lecteurs de cartes PC/SC sont nécessaires pour en assurer la lecture.

Elle est particulièrement utilisée par le fournisseur de services « feuille de soins électronique » (FSE), à la fois pour l'identification électronique et la signature.

Elle permet, par transitivité de s'activer une application mobile e-CPS par CPS (https://wallet.esw.esante.gouv.fr/)

4.2.2.4. Le moyen d'identification électronique « application mobile e-CPS »

La e-CPS permet à un professionnel de s'authentifier auprès de services en ligne en utilisant une application mobile disponible sur smartphone ou tablette (détention : 1er facteur), avec la saisie d'un code PIN (connaissance : 2ème facteur). L'authentification permise par e-CPS est d'un niveau de sécurité équivalent à l'authentification par carte CPS.

L'application e-CPS peut être activée par transitivité par CPS ou par fourniture de deux secrets sur des canaux différenciés (e-mail et téléphone portable) et validés lors de l'enregistrement du professionnel chez le FI ANS par les autorités d'enregistrement, ou mis à jour après une identification électronique par Pro Santé Connect (ou, transitoirement, par les systèmes d'identification électronique mis en place par les ordres professionnels).

Tous les professionnels enregistrés au RPPS peuvent bénéficier de ce MIE.

Ce MIE fera l'objet de réactivations régulières, à minima tous les trois ans.

À janvier 2020, presque 100 000 e-CPS ont été activées, principalement tirées par les usages autour des fournisseurs de services SI-DEP et Vaccin Covid.

4.2.2.5. Le fédérateur Pro Santé Connect (PSC)

Pour faciliter la mise en œuvre de l'identification électronique, l'Etat propose un **fédérateur de moyens d'identification électroniques** similaire à France Connect pour les usagers.

Il intègre la carte CPS ou la e-CPS. D'autres FI/MIE pouvant être ajoutés ultérieurement, voire France Connect qui pourrait y être implémenté dès qu'un mécanisme de chaînage fiable avec les données sectorielles du RPPS sera trouvé.

Basé sur le standard Open ID Connect, il décharge les FS de l'implémentation des MIE et permet de « servir » l'identité sectorielle des répertoires de référence (profession, exercices, etc.) aux fournisseurs de services.

À novembre 2020, une cinquantaine de FS, dont certains utilisés pour la gestion de la crise sanitaire Covid-19 (SI-DEP, Vaccin Covid, Santé.fr notamment), implémentent PSC.

Ce fédérateur permet une navigation entre FS fluide pour les usagers, sans apparente réidentification électronique.

En 2021, il deviendra disponible pour les services non-web (clients lourds / application mobiles) via le protocole CIBA[41] d'Open ID. Il intègrera une possibilité de déconnexion et améliorera significativement sa documentation et ses interfaces utilisateurs.

SYNTHESE DES ACTIONS CLES

Action	Jalon
Publication de l'arrêté d'expérimentation sur l'élargissement du RPPS	Février 2021
Intégration de PSC dans le volet TLSi AMO du CI-SIS	S1-2021
Disponibilité de PSC pour les usages clients lourd / applications mobiles via le protocole CIBA	T2-2021
Nouveau décret RPPS+, élargissant le répertoire à l'ensemble des acteurs intervenant en santé	T3 2021
Premier arrêté e-CPS et premier arrêté Pro Santé Connect	T3 2021
Publication arrêté « référentiel identification électronique des ASPP », après concertation	T4 2021
Bascule de l'enregistrement des infirmiers au RPPS	Septembre/Octobre 2021
Décommissionnement complet de l'application ADELI	Fin 2022
Atteinte d'un niveau minimum de garantie « renforcé » pour l'IE des ASPP	1er janvier 2023
Intégration de PSC pour l'IE des ASPP	1er janvier 2023
Atteinte d'un niveau garantie équivalent substantiel pour l'IE des ASPP : Pro Santé Connect (PSC) et/ou dispositif d'IE substantiel eIDAS et/ou dispositif d'IE certifié CSPN ANSSI	1er janvier 2026

[41] https://openid.net/tag/ciba/

SYNTHESE DES IMPACTS POUR LES MOE ET MOA

Synthèse des impacts pour les MOA (Structures de santé, GRADeS…)

- Accompagnement de l'enregistrement des professionnels, voire enregistrement via ENREG
- Mise à jour des politiques de sécurité locales sur l'identification électronique
- Actions vis-à-vis des éditeurs pour implémentation Pro Santé Connect, avec éventuellement en complément des FI (SSO/IAM/etc.) au niveau renforcé

Synthèse des impacts pour les MOE (Industriels)

- Intégration de Pro Santé Connect et/ou de nouvelles solutions d'IE, davantage sécurisées
- Intégration des couches d'exposition du RPPS

POUR EN SAVOIR PLUS

https://esante.gouv.fr/securite/e-cps

https://esante.gouv.fr/securite/e-cps/services-raccordes-a-pro-sante-connect

https://annuaire.sante.fr/

https://annuaire.sante.fr/web/site-pro/extractions-publiques

https://esante.gouv.fr/interoperabilite/mos-nos

4.2.3. Identité électronique des Acteurs de Santé Personnes Morales (ASPM)

Les services numériques de santé concernés par ce présent cadre de référence sont les **services traitant des données de santé à caractère personnel, au sens du RGPD**[42]**.**

DOCTRINE

4.2.3.1. Niveau de garantie cible des fournisseurs d'identité intégrés par les fournisseurs de service

Au 1er janvier 2023 (dans 2 ans), il est attendu, pour les services numériques partagés qu'ils implémentent pour l'IE des ASPM des certificats de l'autorité IGC-Santé. Les services à usage interne à une communauté fermée peuvent aussi implémenter d'autres types de certificats

Les certificats sont contrôlés par les FS (liste ou API d'opposition = CRL / service OCSP, date de validité, etc.).

Un FS peut demander la transmission de données complémentaires, par exemple au travers d'un jeton Open ID ou SAML2.0, comme l'identité de la personne physique ou du processus automatique à l'origine de la transaction, ou l'identifiant de la politique de sécurité locale. L'identification « indirecte » n'est néanmoins pas recommandée : **soit une personne physique est identifiée électroniquement, soit c'est une personne morale,** qui est alors responsable de la gestion de son identification interne (personnes et processus), de son contrôle et de la traçabilité.

L'IGC Santé sera incluse au S1 2021 dans le volet TLSi AMO du CI-SIS.

4.2.3.2. Les répertoires de référence FINESS et SIREN/SIRET

Les certificats IGC-Santé contiennent l'identifiant à portée nationale, vérifié à l'enrôlement.

À l'occasion de l'identification électronique, les FS ont l'obligation de référencer l'identifiant de portée nationale. Ce dernier doit être « servi » par le FI / MIE. Grâce à cet identifiant, le FS peut aller chercher des données complémentaires (type de structure, etc.) sur des couches d'exposition.

L'enrôlement à l'IGC-Santé passe par une contractualisation unique au niveau des structures juridiques.

Les identifiants de portée nationale peuvent être :

- En priorité, l'identifiant FINESS géographique (de préférence) ou juridique ;
- Les SIREN et SIRET attribués par l'INSEE ;
- De façon transitoire RPPS_RANG et ADELI_RANG et éventuellement l'identifiant « répertoire national des associations » (RNS) pour les ESMS notamment.

Le répertoire FINESS verra en 2021 un cadrage stratégique sur sa rénovation fonctionnelle et technique, et l'arrêté FINESS sera revu, en application de l'ordonnance identification électronique.

Dérogatoirement, les identifiants peuvent également être de portée locale pour les usages au sein d'une communauté fermée, établis par une autorité d'affectation.

SYNTHESE DES ACTIONS CLES

[42] https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

Action	Jalon
Intégration de l'IGC Santé dans le volet TLSi AMO du CI-SIS	S1 2021
Publication arrêté « référentiel identification électronique des ASPM », après concertation	T4 2021
Publication d'un arrêté sur les certificats de personnes morales IGC-Santé	S2 2021/S1 2022
Refonte arrêté FINESS	S2 2021
Utilisation des moyens d'IE autorisés (certificats de personne morale de l'autorité de certification de référence : l'IGC-Santé) pour les personnes morales	1er janvier 2023

SYNTHESE DES IMPACTS POUR LES MOE ET MOA

Synthèse des impacts pour les MOA (Structures de santé, GRADeS…)

Contractualisation avec l'ANS (IGC-Santé) pour la délivrance de MIE certificats

Synthèse des impacts pour les MOE (Industriels)

Intégration des certificats IGC-Santé pour l'identification électronique

Intégration des couches d'exposition du FINESS

POUR EN SAVOIR PLUS

http://igc-sante.esante.gouv.fr/PC/
http://finess.sante.gouv.fr/fininter/jsp/rechercheSimple.jsp?coche=ok
https://www.data.gouv.fr/fr/datasets/finess-extraction-du-fichier-des-etablissements/
https://www.data.gouv.fr/fr/datasets/base-sirene-des-entreprises-et-de-leurs-etablissements-siren-siret/

4.2.4. Des grandes orientations transversales sur les contrôles d'accès

Les contrôles d'accès sont définis par le FS, si possible indépendamment des attributs de l'IE. Ils sont paramétrés avec des schémas par défaut propres à chaque service et complétés par des ouvertures/fermetures (liste blanche / liste de noire) de (groupes de) personnes, professionnels et services numériques, selon des périmètres de données variés (*scopes*), temporaires ou permanentes, transitives ou non par délégations successives de droits d'administration (délégation de droits d'un professionnel à un autre).

Les patients doivent devenir, autant que possible, les administrateurs des contrôles d'accès les concernant, qu'il s'agisse d'accès par leurs proches, les professionnels qui les prennent en charge ou les services numériques référencés dans l'ENS.

À terme, un répertoire national des contrôles d'accès pilotés par le patient pourrait être mis en place dans le cadre de l'ENS, basé sur la technologie UMA2.0 (dérivé de OAuth2.0). Cela permettra au patient de vraiment exprimer les autorisations d'accès, avec le principe « dites-le nous une fois », et aux FS d'externaliser tout ou partie de la gestion des CA auprès de l'ENS, par exemple pour la réutilisabilité des données de santé pour la recherche.

L'articulation avec un référentiel des « équipes de soins », souvent défini au niveau d'un établissement ou dans les SI régionaux devra être étudié. Les sujets spécifiques associes aux autorisations conférées aux personnes morales devront également être investigués.

4.2.5. Signature électronique

La signature électronique permet notamment de garantir aux destinataires de documents de santé leur intégrité, leur origine et leur non-répudiation, au travers de l'utilisation des outils de vérification adéquats. Cela permet de partager des documents en toute confiance et de valider l'authenticité de certains documents essentiels (résultats de biologie médicale, etc.).

Des échanges menés courant 2021 avec l'écosystème permettront d'étudier l'opportunité pour la puissance publique :

- De lancer un service national de signature de documents, adossé à une identification électronique basée sur Pro Santé Connect et des certificats IGC-Santé pour les personnes morales ;
- D'organiser une labellisation de solutions industrielles de signatures conforme à des exigences à définir.

En attendant, il est recommandé de prendre connaissance :

- Du référentiel « force probante des documents de santé » qui sera publié en version post-concertation en février 2021 (introduction, annexe numérisation, annexe production, annexe matérialisation, annexe métadonnées, annexe classification) ;
- De la partie signature électronique du règlement eIDAS ;
- À l'initiative « e-Signature » du mécanisme pour l'interconnexion en Europe / Connecting Europe Facility (CEF), des standards XAdES, CAdES, PAdES et ASiC compatibles aux normes européennes sur la e-Signature ;
- Des différentes offres du marché ou, pour monter sa propre infrastructure, la librairie « Digital Services Signatures » (DSS), par exemple mise en place par l'ANS à travers eSignSante pour ses propres besoins.

4.2.6. Un dispositif d'accompagnement

Dans le cadre du Ségur de la Santé, un dispositif pourrait être mis en place à l'Agence du Numérique en Santé courant 2021-2022 pour accompagner les utilisateurs dans leurs questions sur l'IE et les CA, et notamment dans :

- La mise en œuvre de PSC pour les FS ;
- L'interrogation des couches d'exposition du RPPS et de FINESS ;
- L'enregistrement des professionnels dans le RPPS (via portail ENREG) pour les nouvelles autorités d'enregistrement ;
- La mise en place de solutions d'IE privées au sein des structures (SSO, IAM, etc.) et leur certification en lien avec les éditeurs concernés ;
- L'interfaçage avec les outils de gestion du cycle de vie des cartes ;
- Les solutions de signature électronique, par exemple de type eSignSante, et de contrôle de signatures ;
- La formalisation de règles de CA.

4.3. Sécurité opérationnelle

DOCTRINE

Pour garantir la confiance dans la e-santé, la sécurité opérationnelle des systèmes numériques en santé doit être renforcée tant au niveau réactif que préventif au travers :

- D'une extension de l'obligation de déclaration des incidents de sécurité, à l'ensemble des structures sanitaires et médico-sociales (sur la base de l'existence d'un référencement FINESS) ;
- De l'obligation pour l'ensemble des structures du secteur sanitaire puis du secteur médico-social, qui ont un ou plusieurs systèmes exposés sur Internet, de se soumettre à un audit annuel de leur exposition sur Internet en vue de détecter de façon préventive les vulnérabilités exposées en vue d'améliorer la couverture des risques cyber ;
- Dans le même esprit de renforcement du niveau de sécurité des structures sanitaires et médico-sociales celles-ci devront faire réaliser un audit annuel de leurs infrastructures internes ;
- D'une coordination avec l'initiative européenne en matière de cybersécurité et cybersurveillance.

Par ailleurs, l'ANS a pour objectif d'être reconnue comme CSIRT (Computer Security Incident Response Team) étatique pour le secteur santé et médico-social, reconnaissance lui accordant une plus grande légitimité auprès de l'ensemble des acteurs dans la mise en œuvre de ses actions de prévention.

❶ Extension du dispositif de déclaration des incidents de sécurité

Ce dispositif de signalements constitue le premier maillon de la cybersécurité du secteur sanitaire et médico-social, en contribuant à repérer les attaques avant qu'elles ne se répandent et à renforcer ainsi la capacité de réponse collective.

Le suivi de l'évolution de la menace cyber et l'expertise nécessaire pour faire face à un acte de cyber-malveillance nécessitent la mise en place de moyens trop importants pour de nombreuses structures. Par ailleurs, les prestations de veille et d'expertise en cybersécurité (aide à la réponse à un incident de sécurité et renforcement de la sécurité à la suite de cet incident) s'avèrent souvent trop onéreuses pour les structures de taille modeste.

Au-delà de l'obligation de déclaration, le ministère propose au travers de la cellule ACSS un véritable service aux structures de santé, à la fois dans le cadre du traitement de leurs incidents, mais aussi en vue de renforcer les actions préventives pour en limiter les occurrences. L'enjeu principal est de soutenir et d'accompagner la démarche eSanté, par une démarche de sécurité forte et visible, de nature à apporter la confiance nécessaire aux patients / usagers et aux acteurs de santé.

Le dispositif ministériel de prévention et d'alerte, s'articule autour du portail "cyberveille-sante.gouv.fr", conçu pour informer sur les menaces numériques qui pèsent sur le secteur (veille sectorielle), donner aux acteurs les clés pour y faire face et partager les pratiques au sein d'un espace sécurisé.

L'extension de l'obligation de déclaration à l'ensemble des structures de santé et du médico-social (sur la base de l'existence d'un référencement FINESS) doit permettre d'accompagner l'ensemble des structures du secteur et en particulier d'apporter un appui aux structures les plus vulnérables afin d'améliorer leur résilience face à la menace cyber et ainsi participer au décloisonnement entre ces structures.

La mise en place d'un **observatoire des incidents** (dispositif national centralisant la remontée des incidents impactant l'ensemble du territoire) apporte une vision consolidée de la menace au niveau sectoriel. Il fournit des éléments de pilotage sectoriel de la sécurité, permet d'identifier les efforts à réaliser (nécessaires) en matière de sécurité opérationnelle (en fonction des incidents survenus). Il offre également l'opportunité de détecter les menaces sectorielles et de freiner leur exploitation généralisée en alertant le réseau des correspondants.

L'observatoire produit des analyses sectorielles de la sécurité, fondées sur le traitement des signalements d'incidents de sécurité, complétés le cas échéant, par des études et/ou veilles complémentaires. Il propose des axes d'amélioration de la sécurité opérationnelle fondés sur les retours d'expérience des incidents signalés ainsi que les statistiques consolidées d'évènements.

❷ Obligation de mise en œuvre d'un audit des systèmes exposés sur Internet

Un grand nombre d'incidents de cybersécurité sont la conséquence de l'exploitation malveillante de vulnérabilités de systèmes exposés sur Internet. L'interconnexion croissante des systèmes des acteurs de santé est un facteur supplémentaire de propagation des actes de cyber-malveillance et de leur impact systémique potentiel.

La réalisation d'un audit de l'exposition sur Internet est rendue obligatoire pour l'ensemble des structures sanitaires et médico-sociales afin que soit mis en place les solutions permettant de réduire les principaux risques de sécurité.

Un audit de l'exposition des systèmes sur Internet doit **mesurer le degré d'exposition des interfaces** exposées d'un système au regard des vulnérabilités connues, de l'état de l'art, …

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**. Il doit être complété par un audit de l'infrastructure interne de l'établissement voire des équipements biomédicaux.

L'audit de l'exposition des systèmes sur Internet consiste à :

- Cartographier et déterminer la surface d'attaque d'un système d'information ;
- Détecter de manière pro-active les vulnérabilités qui affectent le système d'information d'une organisation ;
- Détecter une éventuelle fuite de données (fuite de code-sources, fuite de données, fuite de données utilisateur, etc.) visant le système d'information.

Le rapport de cybersurveillance fourni présente l'ensemble des vulnérabilités détectées par criticité ainsi qu'un plan d'actions de remédiation hiérarchisé.

Il doit être mis en œuvre au moins une fois par an afin de : :

- Tenir compte de l'apparition fréquente **de nouvelles failles** ;
- Et mesurer les **efforts de correction** en restituant l'évolution de l'exposition à la menace cyber pour le périmètre considéré.

Cet audit peut être réalisé par l'ANS (au travers de son service national de cybersurveillance) ou par un prestataire spécialisé dans les audits techniques de cybersécurité.

L'ANS (Cellule ACSS) constitue un **observatoire des vulnérabilités** sur la base d'une consolidation des rapports de cybersurveillance unitaires.

L'observatoire fournit une analyse de l'exposition sectorielle (benchmark), par typologie de vulnérabilités, par type de structures, …, et mesure son évolution dans le temps.

❸ Renforcement du niveau de sécurité des structures de santé par un audit de l'infrastructure interne

Pour renforcer la résilience des structures de santé vis-à-vis des cybermenaces, l'audit de l'exposition des systèmes sur Internet doit être complété par une évaluation de la sécurité de l'infrastructure interne et la mise en œuvre progressive de mesures visant à réduire l'impact d'une activité potentiellement malveillante en son sein.

Il est recommandé de faire auditer au minimum les services suivants :

- L'« Active Directory », colonne vertébrale du SI (gestion de l'annuaire, de l'authentification et des droits d'accès, de la politique logicielle, de la résolution des noms, etc….) : l'ANSSI propose un outil utilisable librement et un appui dans sa mise en œuvre; L'ANS va monter en compétence sur cet outil en 2021 et sera en mesure d'apporter également un appui à partir du 2ème semestre ;
- La messagerie électronique qui constitue le premier vecteur d'introduction d'une activité malveillante au sein d'un système d'information : l'ANS propose un service de tests de la politique de contrôle des messages et de leur contenu (usurpation d'identité, pièce jointe malveillante (spam, virus, etc…), URL malveillante (hameçonnage), etc…).

❹ Reconnaissance de l'ANS (Cellule ACSS) comme CSIRT (Computer Security Incident Response Team) étatique pour le secteur santé et médico-social

La Cellule ACSS va intégrer d'ici la fin de l'année l'InterCERT-FR avec l'appui de l'ANSSI et se positionner comme CSIRT étatique (Computer Security Incident Response Team) pour les acteurs sanitaires et médico-sociaux. La reconnaissance de ses activités d'appui à la réponse aux incidents de sécurité et à la prévention de la menace, par ses pairs, permettra de :

- Bénéficier des retours d'expérience et de la coopération avec les autres CSIRT/CERT en vue d'améliorer ses services au profit des structures de santé ;
- Développer la confiance des acteurs de santé en améliorant la qualité des processus.

TRAJECTOIRE

❶ Extension du dispositif de déclaration des incidents de sécurité

Le dispositif de signalement des incidents de sécurité est étendu à l'ensemble des structures de santé et du secteur médico-social ainsi qu'en cible, aux dispositifs connectés.

Les modalités d'accompagnement de l'ensemble des structures du secteur doivent être prévues en conséquence.

Les incidents remontés alimentent l'observatoire des incidents.

En outre, l'extension du circuit de diffusion des signalements doit être étendu vers les autorités compétentes de l'Etat en fonction de la nature de l'incident (vers la CNIL ou l'ANSSI en tant que de besoin). Cette extension doit permettre aux structures de faire une seule déclaration.

❷ Mise en place d'un référentiel d'audit de l'exposition sur Internet

Un référentiel d'audit de l'exposition des systèmes sur Internet doit être publié pour encadrer la réalisation des audits. Il doit préciser la nature de l'ensemble des tests à réaliser.

Pour être opposable, l'obligation pour les structures de faire auditer leur exposition sur Internet doit faire l'objet d'une mise à jour au sein de la réglementation relative aux obligations de sécurité des systèmes d'information.

❸ Mise en place d'un service en ligne de commande d'audit de cybersurveillance

L'ANS va mettre en place une plateforme permettant de commander en ligne des audits de son exposition sur Internet et ainsi d'automatiser le processus de demande d'audit et de restitution des résultats. De nombreux tests seront également automatisés. Cela permettra d'augmenter significativement le nombre d'audits pouvant être réalisés simultanément.

❹ Mise en place d'un service en ligne de test de la sécurité de son domaine de messagerie

L'ANS va mettre en place une plateforme permettant de tester en ligne la sécurisation de son domaine de messagerie et de proposer un rapport avec un plan d'action pour améliorer la configuration des règles de sécurité.

❺ Intégration définitive de la cellule ACSS au sein du groupe « Inter CERT »

Pour intégrer définitivement l'InterCERT-FR, la Cellule ACSS doit atteindre le niveau de maturité basique SIM3 (Security Incident management Maturity Model - ENISA) dans ses pratiques quotidiennes de CSIRT au cours de sa première année de participation. Une évaluation a été réalisée en juillet 2020 et un plan d'action a été établi pour mettre en place les mesures nécessaires en vue d'atteindre ce niveau de maturité avant juillet 2021.

❻ Inscription dans la loi du rôle et des missions de CSIRT de l'ANS (Cellule ACSS) au profit des acteurs sanitaires et médico-social

Le cadre réglementaire concernant le rôle et les missions de l'ANS (Cellule ACSS) dans le dispositif de signalements des incidents de sécurité doit être révisé afin de prendre en compte l'évolution de ses activités au profit des acteurs sanitaires et médico-sociaux.

Dans le cadre d'une croissance significative de la menace de cybersécurité sur Internet, la Cellule ACSS a développé une plateforme permettant d'alerter les structures de façon proactive lorsqu'elles exposent un système vulnérable sur Internet. La Cellule ACSS a constitué une base d'information permettant d'identifier les structures de santé sur Internet (IP et noms de domaine) ainsi qu'une cartographie des serveurs exposés. Pour pérenniser la mise en œuvre de ce service de prévention de la menace et d'incitation à la correction des vulnérabilités, il doit faire l'objet d'un encadrement réglementaire légitimant les actions d'audits passifs (de recherches ciblées) de l'ANS.

SYNTHESE DES ACTIONS CLES

Le tableau ci-après présente une vue synthétique des actions et les échéances associées.

Action	Jalon
Extension du dispositif de déclaration des incidents	2021
Publication d'un référentiel d'audit de l'exposition des systèmes sur Internet	2021
Mise en place d'une plateforme de commande d'audit en ligne	2021
Mise en place d'un service en ligne de tests de son domaine de messagerie	2021
Reconnaissance de la cellule ACSS au sein du groupe InterCERT-FR	2020 - 2021
Inscription dans la loi du rôle et des missions de CSIRT de l'ANS (Cellule ACSS) au profit des acteurs sanitaires et médico-social	2021

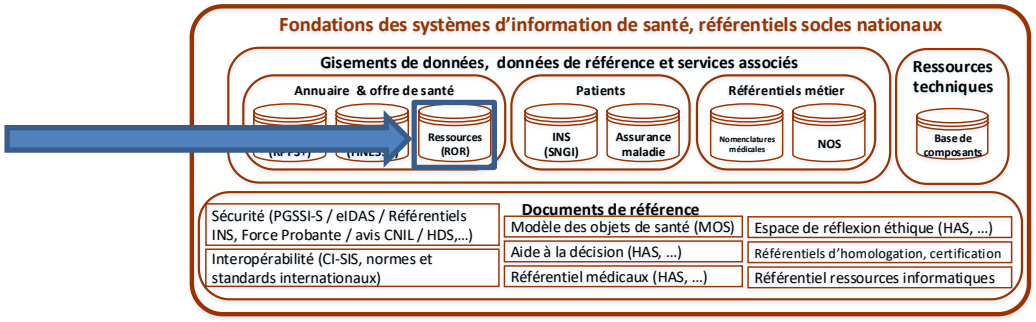
SYNTHESE DES IMPACTS POUR LES MOE ET MOA

Synthèse des impacts pour les MOA (Structures de santé, GRADeS…)	Synthèse des impacts pour les MOE (Industriels)
Réalisation : ▪ D'un audit de l'exposition sur Internet (pour l'ensemble des structures sanitaires et médico-sociales) ▪ D'une analyse de sécurité de l'ensemble des actifs numériques (action du responsable de traitement) ▪ D'un audit de l'infrastructure interne de l'établissement voire des équipements biomédicaux (notamment active directory et services de messagerie) ▪ D'un plan d'actions correctif	Mise en œuvre du plan d'action correctif de failles identifiées par les MOA lors des différents audits réalisés

POUR EN SAVOIR PLUS

- Accompagnement Cybersécurité des Structures de Santé :
  - https://esante.gouv.fr/securite/accompagnement-cybersecurite-des-structures-de-sante
- *Fiches réflexes par type de menaces accessible à travers le portail Cyberveille-Santé :*
  - https://www.cyberveille-sante.gouv.fr/
- Observatoire des signalements des incidents de sécurité des systèmes d'information pour le secteur santé :
  - https://esante.gouv.fr/media/2530
- Initiative européenne en cybersécurité : https://ec.europa.eu/digital-single-market/en/cyber-security

5 – Offre de santé



Le Répertoire Opérationnel des Ressources (ROR) constitue le référentiel de données de description de l'offre de santé commun aux secteurs sanitaire et médico-social. Il a vocation à offrir une description exhaustive, homogène et opérationnelle de l'offre de santé sur le territoire national afin d'alimenter les applications métier qui facilitent l'orientation et la mise en œuvre d'un parcours usager fluide.

DOCTRINE

❶ Le ROR constitue le référentiel unique de données de description de l'offre de santé, commun aux champs sanitaire et médico-social

Le ROR constitue le **référentiel unique de données de description de l'offre de santé** portée par les structures qui participent au rétablissement ou à l'entretien de la Santé d'une personne tout au long de son parcours de santé. **Il est commun aux champs sanitaire et médico-social**.

Ce référentiel alimente les applications métiers, utilisées par des professionnels ou des usagers, qui contribuent à l'orientation des personnes (exemple : Viatrajectoire, sante.fr, SI-Samu) ou à la coordination des parcours de santé (exemple : services numériques de coordination destinés aux dispositifs d'appui à la coordination et aux professionnels participant aux communautés professionnelles territoriales de santé).

Le ROR leur permet de bénéficier d'une description de l'offre de santé unique et homogène. **La qualité des données du ROR est donc stratégique pour assurer la qualité des prises en charge et des orientations, via leur usage par l'ensemble des applications qui s'appuient sur ce référentiel**.

Son périmètre actuel, **fixé nationalement**, couvre l'offre de santé portée par les établissements sanitaires (MCO, SSR, PSY), par les établissements et services en charge des personnes âgées en perte d'autonomie (PA) et des personnes en situation de handicap (PH) et les structures de ville (cabinets libéraux, maisons de santé, centres de santé). Ce périmètre évolue en fonction des besoins exprimés par les utilisateurs.

❷ Le ROR présente une description unifiée de l'offre de santé

L'offre de santé se définit comme un ensemble de soins ou de services dispensés par une structure de santé (un établissement sanitaire, un établissement médico-social, une structure de ville).

Les établissements sanitaires et médico-sociaux décrits dans le ROR sont identifiés à partir du FINESS (fichier de référence national des établissements sanitaires et sociaux) et les cabinets libéraux à partir du RPPS (répertoire partagé des professionnels de santé), afin de garantir l'interopérabilité avec de nombreux systèmes.

Ces données d'identification sont ensuite complétées par la description des activités opérationnelles délivrées par la structure, et des ressources opérationnelles mises en œuvre pour réaliser ces activités :

- La capacité d'accueil pour cette activité (capacité et disponibilité en lits et places) ;
- Les équipements spécifiques pour réaliser les activités opérationnelles ;
- Les professionnels de santé qui contribuent à ces activités et peuvent être contactés.

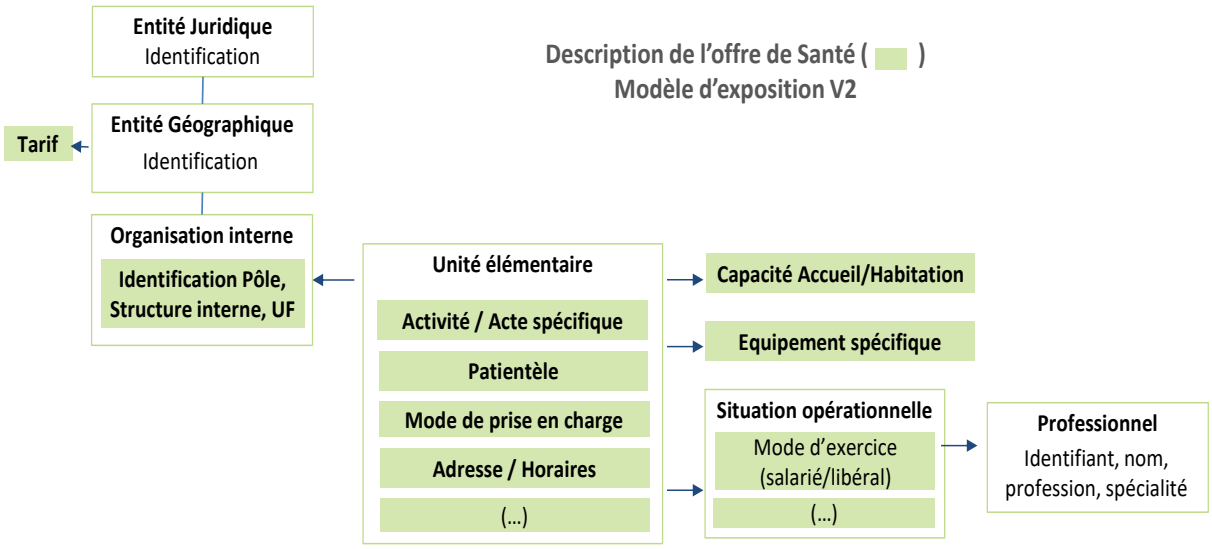
Ce niveau de description opérationnel est saisi manuellement ou alimenté automatiquement par les établissements et structures qui portent l'offre de santé.

Le ROR présente et diffuse l'offre de santé aux applications via un **modèle d'exposition**[43] des données, commun pour l'ensemble des offres sanitaire et médico-sociale. Ce modèle d'exposition normalise la description des structures sur l'ensemble du territoire et sur les champs sanitaire et médico-social. Le socle de données qui doit être alimenté dans **le modèle d'exposition est fixé au niveau national.**

Certaines données du modèle d'exposition sont définies avec des valeurs normées appelées nomenclatures. Ces nomenclatures permettent d'homogénéiser la description de l'offre sur le territoire et de faciliter la recherche. Ces jeux de valeurs sont définis dans des groupes d'experts au niveau national et évoluent avec les besoins métiers.

Le modèle présenté ci-dessous est volontairement simplifié pour faciliter la lecture :

[43] Le modèle d'exposition présenté dans ce document est volontairement simplifié. Le modèle complet est accessible sur le lien ci-contre : https://esante.gouv.fr/projets-nationaux/repertoire-operationnel-ressource. Le modèle d'exposition décrit l'organisation des données de descriptions de l'offre. Il structure ces données, c'est-à-dire qu'il les hiérarchise, les ordonne et les type.



Les données présentées via le modèle d'exposition ne sont pas opposables au sens juridique du terme[44]. En revanche, certaines données sont soumises à des contraintes réglementaires (règles qui régissent les référentiels nationaux, RGPD pour les données personnelles) et à des obligations de qualité.

❸ La consommation de données du ROR implique de s'inscrire dans l'espace de confiance du ROR et de respecter un ensemble d'engagements

L'architecture actuelle du ROR est une architecture distribuée. Deux solutions techniques, appelées solution ROR, sont implémentées en région. **Chaque ARS met en œuvre et exploite une des deux solutions ROR. Elle est responsable du peuplement du référentiel sur le périmètre régional[45]**, sans intersection de périmètre entre les régions. L'ensemble des ROR régionaux fournit ainsi une vision nationale de l'offre de santé.

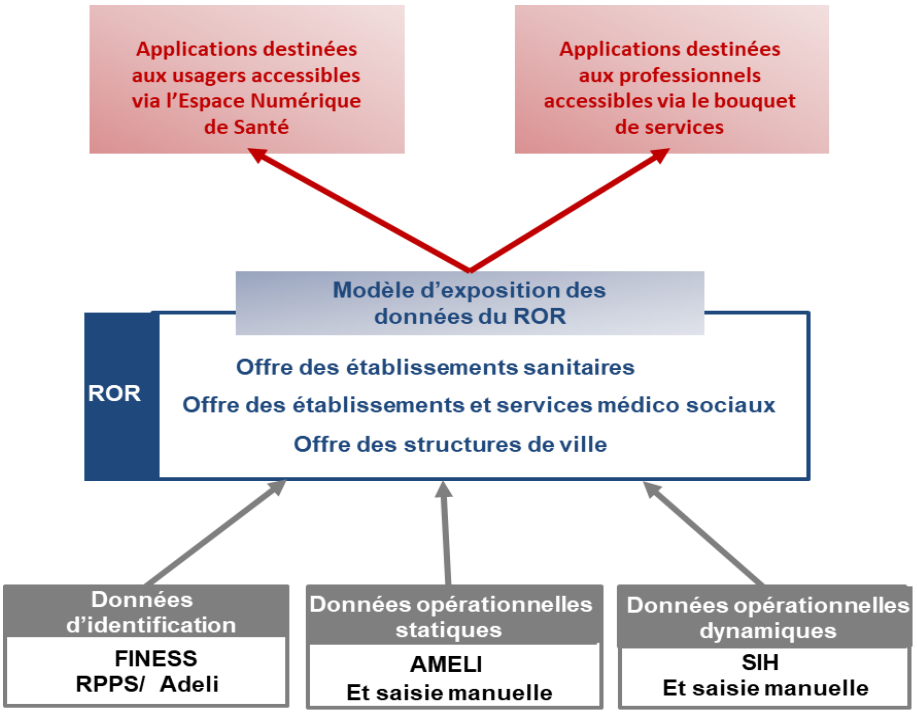
En termes d'usage, toute application, accessible via l'espace numérique de santé ou le bouquet de services aux professionnels, qui vise à faciliter l'orientation, la régulation, la coordination et l'information des acteurs, peut utiliser les données de n'importe quel ROR régional via des transactions normalisées[46]. Pour ce faire, elle doit s'inscrire dans **l'espace de confiance du ROR et respecter des engagements techniques, de sécurité et de bon usage des données**[47].

[44] La notion juridique d'opposabilité des données repose sur une présomption de validité de celles-ci du fait de leur contrôle par une autorité d'enregistrement sur la base de pièces justificatives. Les données du ROR sont sous la responsabilité du directeur de la structure et sous le contrôle de l'ARS, sans répondre toutefois aux critères d'opposabilité juridique ; pour les données « dynamiques », la vigilance de l'utilisateur s'impose pour s'assurer de la mise à jour des données (ex. : disponibilité des lits avant d'orienter un patient).

[45] L'ARS est responsable d'organiser le peuplement du ROR, et le directeur de la structure est responsable de l'exactitude des données saisies pour sa structure.

[46] Cadre de référence Programme ROR – Spécifications « modalités d'accès aux ROR » : https://esante.gouv.fr/projets-nationaux/repertoire-operationnel-ressource)

[47] Cadre de référence - Doctrine d'urbanisation du ROR – Annexe « espace de confiance du ROR » : https://esante.gouv.fr/projets-nationaux/repertoire-operationnel-ressource



TRAJECTOIRE

❶ Consolider le périmètre de description de l'offre pour répondre aux usages

Le peuplement des ROR doit se poursuivre en tenant compte du respect du critère d'exhaustivité de la description de l'offre, avec pour objectif d'ici 2022 :

- La finalisation du peuplement conformément au périmètre fixé pour les établissements de santé ;
- La généralisation du peuplement sur le champ médico-social, démarré depuis 2019 ;
- L'initialisation de la description de l'offre de télémédecine, disponible en 2021 ;
- L'initialisation du peuplement de l'offre de ville, dès fin 2020.

L'intégration de l'offre de ville et de la télémédecine nécessite de finaliser les travaux de nomenclatures de description de l'offre et de poursuivre les travaux techniques pour intégrer des données du RPPS/ADELI et d'AMELI[48] dans les ROR et permettre aux applications de consommer cette offre.

Ce peuplement doit s'accompagner de la mise en place d'un processus de gestion de la qualité des données pour s'assurer de l'homogénéité de description avec les nomenclatures d'échange, de la cohérence des données opérationnelles saisies avec les autorisations délivrées et les reconnaissances d'activité[49], de la mise à jour régulière des données et du traitement des données obsolescentes.

[48] Selon la convention CNAM – ANS : numéro de téléphone du cabinet ; secteur de conventionnement ; acceptation de la carte vitale ; information de planning

[49] Actuellement au travers des CPOM et sous réserve des évolutions à venir en lien avec l'ordonnance de simplification des missions des ARS.

❷ Sécuriser l'accès au ROR pour le rendre plus accessible aux éditeurs et services numériques

La multiplication des usages consommateurs des données du ROR rend obligatoire la mise en œuvre des contrôles nécessaires au respect de la politique d'accès à ces données. En effet, bien que le ROR ne contienne aucunes données de santé, la réglementation sur les données personnelles[50], le caractère confidentiel ou très technique de certaines données nécessitent de qualifier l'accès aux données du ROR en fonction du rôle métier des acteurs[51].

Cette garantie de protection des données personnelles et confidentielles repose sur la mise en œuvre technique, par les solutions ROR et les applications consommatrices, des modalités de contrôle d'accès aux données du ROR.

❸ Faire évoluer l'architecture du ROR pour améliorer le niveau de services

L'augmentation prévisible du nombre d'applications consommatrices, dont certaines stratégiques telles que les services numériques de coordination introduits par le programme e-Parcours, ou critiques telles que le SAS ou le SI-Samu, entraine des exigences croissantes vis-à-vis du ROR en termes de niveau de services.

Après étude et concertation des ARS, des GRADeS et des principaux consommateurs de données, le comité de pilotage national ROR a validé début 2020 la mise en œuvre d'un ROR national qui devra assurer un service de consommation des données du ROR à haute disponibilité, évolutif et pérenne en tenant compte de la densité des urbanisations régionales (à l'heure actuelle, 29 applications externes consomment des données du ROR). Ce **scenario de mise en œuvre d'un ROR national** comprend :

- Un espace commun à l'ensemble des régions qui contient les données de description de l'offre de santé (« modèle d'exposition ») partagées par l'ensemble des régions. Cet espace permet un accès à la vision nationale de l'offre de santé ;
- **Des espaces régionaux** qui contiennent les données d'offre de santé régionales complémentaires au modèle d'exposition et sont paramétrables par les régions. Ces espaces permettent aux régions de répondre rapidement aux besoins du terrain. Ces types de données ont vocation à être homogénéisées à l'échelle nationale et à intégrer l'espace commun du ROR ;
- **Un service d'accès unique aux** données du ROR qui permettra d'accéder aux données du socle commun et aux données complémentaires régionales.

La transition de l'architecture actuelle – distribuée en 17 ROR régionaux – vers le ROR national unique nécessite une trajectoire progressive pour intégrer les délais d'adaptation des modules et applications connectées au ROR et sécuriser les usages courants durant la phase de construction du ROR national et la centralisation progressive des flux :

- Cette trajectoire passe, dans un premier temps, par l'ajout fin 2022 d'un ROR consolidé aux 17 ROR régionaux existants qui perdurent. Les services métier sont connectés au ROR consolidé qui leur fournit une vision nationale de l'offre sur le modèle d'exposition ;
- Le périmètre du ROR consolidé est progressivement élargi pour contenir les données régionales, complémentaires au modèle d'exposition, dont les applications ont besoin pour fonctionner. L'ensemble des applications est connecté au ROR consolidé lorsque les données qu'elles utilisent y sont disponibles ;

[50] En application du règlement européen de protection des données (RGP) : https://www.cnil.fr/fr/reglement-europeen-protection-donnees.

[51] Cadre de référence – Doctrine d'urbanisation du ROR – Annexe « Politique d'accès aux données du ROR » : https://esante.gouv.fr/projets-nationaux/repertoire-operationnel-ressource

- La saisie est ensuite réalisée directement dans le ROR national et le ROR régional est décommissionné. Le décommissionnement des ROR régionaux est réalisé progressivement en fonction du profil des régions selon un calendrier allant jusque 2025.

Pendant les trois phases de construction un effort important sera réalisé pour maintenir et faire évoluer les solutions existantes afin de répondre aux besoins métiers.

SYNTHESE DES ACTIONS CLES

Action		Jalon
Consolider le périmètre de description de l'offre	Intégration et diffusion d'un premier niveau de l'offre de ville (RPPS/AMELI)	S1 2021
	Intégration de l'offre de téléconsultation et téléexpertise	2021
	Fin de la phase de peuplement intensive et de mise en qualité de l'offre de santé sur le médico-social	2022
Sécuriser l'accès au ROR	Mise en œuvre de l'ensemble des modalités techniques de la politique d'accès aux données du ROR	2021
Améliorer le niveau de service du ROR	Restitution de l'étude d'architecture	Janvier 2020
	Finalisation du cahier des charges fonctionnel et technique du ROR national, sous réserve des prérequis identifiés	Juin 2020
	Sélection du titulaire du marché de construction du ROR National	Fin T3 2021
	Livraison du 1er jalon du ROR national (consolidation des ROR régionaux sur la base du modèle d'exposition pour les applications consommatrices)	S2 2022

SYNTHESE DES IMPACTS POUR LES MOE ET MOA

Synthèse des impacts pour les MOA (Structures de santé, GRADeS…)

- Structures : sous le pilotage des ARS, s'assurer de la mise à jour annuelles des données décrivant son offre de santé (structures sanitaires) ou réaliser une première description lors des sollicitations (ESMS, professionnels exerçant en ville…).
- GRADeS : anticiper les évolutions de l'écosystème régional avec la mise en place du ROR N en participant aux groupes de travail nationaux menés par l'ANS (urbanisation, convergence des données…).

Synthèse des impacts pour les MOE (Industriels)

- Intégrer les principes d'urbanisation du ROR dans ses solutions numériques.
- Intégrer le modèle d'exposition et les spécifications d'alimentation et de mise à jour dans ses solutions numériques.

POUR EN SAVOIR PLUS

https://esante.gouv.fr/projets-nationaux/repertoire-operationnel-ressource

https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/article/repertoire-operationnel-des-ressources-ror

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

Version finale 2020 post concertation publique