AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

LA E-SANTÉ FRANÇAISE HospiConnect

HospiConnect

> ***Vers "Une identité numérique fiable et maîtrisée qui accède aux services numériques en santé"***

Webinaire #0 - HospiConnect#BannièreUnifiée

- Contexte européen & national
- Trajectoire Identification Électronique
- Pourquoi HospiConnect?

13/03/2026

Agence du numérique en santé

Les Intervenants du jour

Florian Catteau
Directeur de Programme
ANS

Joachim Metzger
Directeur de Domaine
ANS

Adeline Lembré
Responsable projets
ANS

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Webinaire, les bonnes pratiques

Je coupe mon micro
(sauf si je suis autorisé à prendre la parole)

Je lève la main
avant de prendre la parole

Activer la caméra **n'est pas nécessaire** pour le bon déroulé du webinaire

Je pose mes **questions** dans **l'espace conversation**

PARCOURS WEBINAIRES

La série de webinaires HospiConnect : un parcours progressif

Cette série de six webinaires a été conçue comme un **parcours structuré et progressif**, permettant aux établissements de santé et à leurs partenaires de monter en compétence étape par étape. Chaque session aborde une facette complémentaire de la démarche HospiConnect. L'objectif est de construire une compréhension solide et actionnable, session après session.

Webinaire #0 - HospiConnect#BannièreUnifiée

AUJOURD'HUI · Pourquoi HospiConnect ? Comprendre le cadre européen et national, la trajectoire Identification Électronique et la raison d'être de la démarche.

Webinaire #1 - HospiConnect#PérimètreOpérationnel

[19/03] · Faites le tour des sujets essentiels à prendre en compte pour comprendre la couverture complète du projet de transformation en établissement et engager votre démarche HospiConnect.

Webinaire #2 - HospiConnect#ServicesSocles IE

[24/03] · Découvrez les évolutions récentes, les points clés à connaître et l'articulation entre les services socles et l'identification électronique pour mener votre projet et définir votre trajectoire.

Webinaire #3 - HospiConnect#ProgrammesDeFinancement

[26/03] · Focus sur le premier jalon à juin 2026 des programmes de financement HospiConnect/HOP'EN2 et HospiConnect/CaRE, point sur les dépenses éligibles et les livrables attendus.

Webinaire #4 - HospiConnect#RIE

[à venir] · Tout savoir sur la version 2 du Référentiel d'Identification Électronique de la PGSSI-S : exigences applicables aux moyens d'identification électronique et mise en œuvre concrète dans l'établissement.

Webinaire #5 - HospiConnect#SNS-DMP-mode AIR Simplifié

[à venir] · Focus sur le Dossier Médical Partagé (DMP) et le mode AIR Simplifié : comprendre les exigences d'accès aux Services Numériques de Santé, les conditions d'alimentation du DMP et la mise en œuvre du mode d'authentification AIR Simplifié en établissement.

💡 **Conseil :** suivez l'intégralité du parcours pour disposer d'une vision complète du contexte stratégique jusqu'aux leviers opérationnels et financiers.

La série de webinaires du Ségur : prochaines sessions

En complément des webinaires HospiConnect, des sessions dédiées aux usages Ségur sont programmées. Elles permettent d'approfondir les cas d'usage concrets liés aux services numériques de santé.

Webinaire Ségur#Consentement à la Consultation du DMP

[Fin mai] · Consentement à la consultation du DMP : comprendre les règles applicables, les modalités de recueil du consentement patient et les impacts sur les pratiques des professionnels de santé en établissement.

Webinaire Ségur#MSS Fonction Réception

[Début juin] · MSS — Fonction réception : maîtriser les exigences liées à la messagerie sécurisée de santé, la fonction réception des documents et son articulation avec le DMP et les services numériques de santé.

💡 **Conseil :** Ces webinaires Ségur sont complémentaires au parcours HospiConnect. Ils approfondissent les cas d'usage concrets des services numériques de santé en établissement..

WEBINAIRE #0

Agenda du jour

Ce premier webinaire est structuré selon une progression logique : nous partons du « pourquoi » (les enjeux et les risques concrets) pour converger progressivement vers le « quoi » (HospiConnect) et le « comment » (ressources et leviers). L'objectif est que chaque participant reparte avec un cadre de compréhension clair et une vision de la trajectoire à engager.

- **Contexte**

  Les enjeux terrain et les risques qui rendent la sécurisation des accès incontournable

  Pourquoi maintenant
  La sécurité sans complexifier
  Cadre Européen
  Cadre National
  Trajectoire de l'Identification Electronique

- **L'Identification Electronique à l'Hôpital**

  Confiance numérique, cybersécurité et protection des données de santé

  Parler le même langage avant de se lancer
  Les réalités terrain
  La réponse : HospiConnect - la bannière unifiée

- **Les composantes HospiConnect**

  La déclinaison opérationnelle sectorielle pour l'hôpital

  Le périmètre opérationnel
  Les services socles de l'ANS
  Le Référentiel Identification Electronique
  Les ressources méthodologiques et les relais terrain
  Les leviers financiers

- **Prochaines étapes**

  Perspectives du webinaire #1

CONTEXTE

Pourquoi la sécurisation des accès est devenue un enjeu majeur

> Le sujet de la gestion des identités et des accès n'est pas un sujet purement technique réservé aux équipes SI. C'est un enjeu de **continuité des soins**, de **confiance des usagers** et de **maîtrise des risques** à l'échelle de l'établissement. Avec l'explosion des services numériques en santé comme le DPI, la télémédecine, les messageries sécurisées, les portails patients, le nombre de comptes utilisateurs et de points d'accès a considérablement augmenté, créant des surfaces d'attaque de plus en plus larges.

Multiplication des accès

Chaque nouveau service numérique génère de nouveaux comptes, de nouveaux mots de passe, de nouvelles portes d'entrée. Sans gouvernance, la complexité devient ingérable.

Risques croissants

Usurpation d'identité, comptes orphelins non désactivés, droits d'accès mal maîtrisés : autant de vulnérabilités exploitées lors de cyberattaques.

Le besoin fondamental

Un accès **sécurisé, fluide et traçable** aux services numériques, sans dégrader les usages quotidiens des professionnels de santé.

Message clé : La sécurisation des accès n'est pas un frein à l'usage. C'est la condition même d'un usage pérenne, confiant et maîtrisé du numérique en santé.

CONTEXTE

Mieux sécuriser, c’est aussi mieux utiliser

> Poser l’enjeu de la sécurisation des accès ne signifie pas annoncer une complexification des usages. Au contraire, l’objectif est de mettre en place des modalités d’accès plus fiables, plus traçables, mais aussi plus fluides pour les professionnels. C’est précisément là que la démarche HospiConnect prend tout son sens.

Protéger

Renforcer la sécurité, c’est protéger vos patients/usagers, vos professionnels et la pérennité de votre système d’information

- Eviter les usurpations d’identité et les accès non autorisés.
- Garantir la traçabilité des actions et l'intégrité des données de santé.
- Réduire les risques d'incidents (cyberattaques, erreurs humaines, fuites de données)

Simplifier

La sécurité n’est pas forcément synonyme d’une expérience utilisateur complexe

- Le renforcement de la sécurité peut s’accompagner d’un gain d’efficience dans l’organisation et d’ergonomie pour les utilisateurs finaux avec des expériences utilisateur pensées pour le terrain. Authentification forte adaptée au contexte (poste de travail, mobilité, urgence).
- Cela peut se traduire par l’utilisation des badges pour s’authentifier sur des solutions de SSO (Single Sign-On) ne nécessitant plus de retenir de multiples mots de passe.

Mettre en conformité

Vous permettre d’être conforme avec la réglementation et impératifs en vigueur

- RGPD
- PGSSI-S RIE
- Secret médical
- La certification HAS

Message clé : mieux sécuriser, c’est mieux protéger sans dégrader les usages.

CONTEXTE

Un cadre européen de confiance numérique qui se renforce

> L'Union européenne a engagé depuis plusieurs années une dynamique visant à construire un socle commun de confiance numérique entre les États membres. Ce cadre s'appuie sur plusieurs textes structurants qui concernent directement le secteur de la santé et renforcent progressivement les exigences en matière de sécurité, d'identification et de gestion des accès aux services numériques.

eIDAS (et eIDAS 2.0) – *Identité numérique et confiance*

Le règlement eIDAS établit le **cadre européen de l'identification électronique et des services de confiance**. Il définit les conditions permettant de reconnaître de manière fiable des moyens d'identification numérique entre États membres et constitue **un socle juridique pour le développement d'identités numériques fortes**.

NIS2 – *Cybersécurité des entités importantes et entités essentielles*

La directive NIS2 **renforce les exigences de cybersécurité applicables aux secteurs hautement critiques**, dont la santé. Elle impose aux organisations des **mesures de gestion des risques et de sécurité renforcée**, dans lesquelles la **maîtrise des identités numériques et des accès aux systèmes** constitue un élément clé.

RGPD – *Règlement Général sur la Protection des Données*

Le RGPD **encadre le traitement des données personnelles,** notamment de santé, sur le territoire de l'Union européenne.
Il **harmonise les règles en Europe** en offrant un **cadre juridique unique** aux professionnels qui leur permet de développer leurs activités numériques favorisant ainsi la confiance des utilisateurs.

EHDS – *European Health Data Space*

L'Espace européen des données de santé vise à **faciliter l'accès et le partage sécurisé des données de santé à l'échelle européenne**. Sa mise en œuvre suppose l'identification fiable des professionnels habilités et la gestion encadrée de leurs droits d'accès aux informations de santé.

Dans ce contexte de renforcement du cadre européen de confiance numérique**, la bannière unifiée HospiConnect** s'inscrit dans une trajectoire visant à sécuriser et simplifier l'identification des professionnels de santé et leur accès aux services numériques, en cohérence avec les exigences portées par eIDAS, NIS2, le RGPD et l'EHDS.

CONTEXTE

Un cadre national structurant pour la santé

> En France, le cadre réglementaire et normatif applicable aux systèmes d'information de santé a considérablement évolué ces dernières années. L'ambition est claire : définir un **langage commun** et des **exigences homogènes** tout en préservant la capacité des établissements à faire leurs propres choix d'organisation et de mise en œuvre technique.

Référentiels de sécurité pour les SI de santé

Un socle commun de règles et de bonnes pratiques s'impose progressivement à l'ensemble des acteurs. Ces référentiels couvrent la gouvernance de la sécurité, la gestion des identités, le contrôle des accès et la traçabilité. Ils constituent le « code de la route » numérique du secteur santé.

Exigences d'identification électronique

Les textes nationaux imposent des niveaux d'assurance croissants pour l'identification et l'authentification des professionnels accédant aux données de santé. L'authentification forte à deux facteurs devient la norme pour les accès aux services numériques en santé.

Convergence vers des usages maîtrisés

L'objectif final n'est pas d'imposer une solution unique, mais de faire **converger les pratiques** vers un niveau de maturité partagé : des identités fiables, des accès gouvernés, et des preuves auditables.

En résumé

Le cadre national traduit les exigences européennes en obligations concrètes pour le secteur santé :

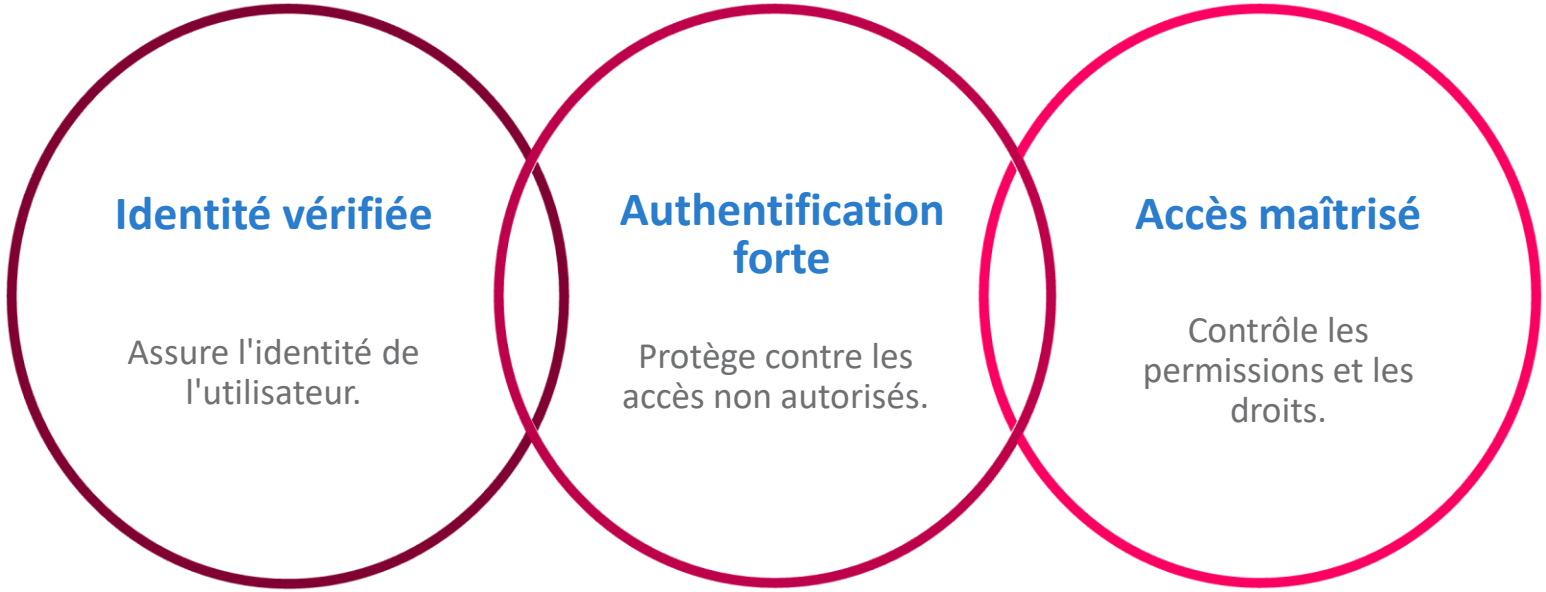
- **Un socle réglementaire** qui s'étoffe et se précise
- **Des référentiels opposables** qui structurent les pratiques
- **Une trajectoire de conformité** progressive et accompagnée
- **Une logique de subsidiarité** : le cadre fixe le cap, l'établissement choisit le chemin

CONTEXTE

Trajectoire IE : une Identité Substantielle de Santé

> L'Identité Substantielle de Santé n'est pas un concept abstrait : c'est un niveau d'assurance défini par le règlement eIDAS et décliné dans la PGSSI-S. Il signifie qu'une identité a été vérifiée de manière rigoureuse, et que l'authentification repose sur au moins deux facteurs. C'est le niveau exigé pour accéder aux services numériques en santé locaux et nationaux (*cf. article 1470 du code de la santé publique*) : DPI, DMP, MSSanté, Pro Santé Connect, etc.

Atteindre le niveau d'assurance « substantiel » pour l'identification électronique de chaque professionnel de santé accédant aux services numériques en santé.



L'enjeu pour les établissements est de construire cette chaîne de bout en bout et de la maintenir dans la durée. HospiConnect fournit le cadre opérationnel pour y parvenir, étape par étape.

CONTEXTE

Les 3 piliers de la gestion des identités et des accès

Gestion des identités

Assurer la bonne prise en compte du cycle de vie des utilisateurs du SI : arrivées, mouvements et départs. Chaque professionnel dispose d'une identité numérique unique, vérifiée et rattachée à son organisation.

Gestion des habilitations

Assurer la bonne affectation des droits d'accès aux applications : gestion des demandes, circuits d'approbation, audit et reporting, revue périodique des accès (recertification). Les habilitations sont attribuées selon le principe du moindre privilège.

Contrôle d'accès

Permettre à un utilisateur d'accéder au service demandé en l'ayant authentifié et autorisé dynamiquement. L'authentification forte à deux facteurs (ce que je sais + ce que je possède) protège l'accès aux services numériques.

Les 3 actions clés

Identification

Saisie d'un identifiant/login ou reconnaissance biométrique. On sait « qui est qui ».

Autorisation

Habiliter une personne à réaliser une action dans le SI : nominative, basée sur un rôle, ou sur le lien entre l'accédant et la ressource accédée.

Authentification

Vérifier qu'une personne est bien celle identifiée à l'aide d'un facteur d'authentification (MIE) : ce que je suis  , ce que je connais  , ce que je possède 

💡 **Ces trois piliers** sont interdépendants : une identité fiable conditionne des habilitations justes, qui conditionnent un contrôle d'accès efficace. C'est la chaîne de confiance numérique en santé.

IE - HÔPITAL

Vocabulaire commun en clair

Avant d'aller plus loin, il est essentiel de partager un **langage commun**. Le domaine de la gestion des identités et des accès regorge de termes techniques qui peuvent générer de la confusion. Voici les concepts fondamentaux, expliqués simplement et illustrés par des exemples concrets du quotidien hospitalier. L'objectif : être lisible et actionnable, sans sacrifier la rigueur.

Terme	Définition simple	Exemple concret
Identité	La personne. C'est le « qui ».	Didier Dupont.
Authentification forte	Comment on prouve son identité. Vérifier qu'une personne est bien celle identifiée à l'aide de facteurs combinés (ex : mot de passe + carte CPS).	Connexion au DPI avec badge + code PIN personnel.
Traçabilité	La preuve des accès et des actions réalisées. Qui a fait quoi, quand, sur quel dossier.	Journal d'accès montrant que le Dr. Dupont a consulté le dossier patient X le 15/03 à 14h32.
Maturité élevée	La capacité de la structure à maintenir un niveau de sécurité opérationnel dans le temps . Procédures établies, responsabilités claires, revues régulières.	Revue trimestrielle des comptes actifs, désactivation automatique après 90 jours d'inactivité.
Gestion des identités	Assurer la bonne prise en compte du cycle de vie des utilisateurs du SI : gestion des arrivées, mouvements et départs.	Création du compte d'un nouvel interne à son arrivée, modification lors d'un changement de service, désactivation à son départ.
Gestion des habilitations	Assurer la bonne affectation des droits d'accès aux applications : gestion des demandes, circuits d'approbation, audit et reporting, revue périodique des accès.	Demande d'accès au DPI validée par le responsable de service, revue trimestrielle des comptes actifs.
Contrôle d'accès	Permettre à un utilisateur d'accéder au service demandé en l'ayant authentifié et autorisé dynamiquement.	Vérification en temps réel que le Dr. Dupont est bien authentifié et habilité avant d'ouvrir le dossier patient.
Données d'identité	Ensemble des traits d'identité permettant d'identifier une personne de manière unique : nom de naissance, liste des prénoms, date et lieu de naissance.	Données d'état civil du Dr. Dupont.
Données sectorielles	Attributs sectoriels associés aux données d'identité : profession, diplôme, lieux d'exercice, identifiants dans les répertoires sectoriels (ex. RPPS).	Spécialité cardiologie, numéro RPPS, établissement d'exercice du Dr. Dupont.
Répertoire d'identité	Base de données ou système d'enregistrement contenant les données d'identité des personnes physiques reconnues dans le cadre d'un schéma d'identification électronique.	L'annuaire LDAP de l'établissement synchronisé avec le RPPS national.
Identification	Saisie d'un identifiant/login par rapport à une base de données.	Saisie du login 'ddupont' à l'ouverture de session sur le poste de travail.
Autorisation	Habiliter une personne à réaliser une action dans le SI : habilitation nominative, basée sur un rôle ou sur le lien entre l'accédant et la ressource accédée.	Un médecin peut consulter les dossiers médicaux mais ne peut modifier que les dossiers de ses propres patients.

Vocabulaire commun en clair

Terme	Définition simple	Exemple concret
Fournisseur de service (FS)	Personne morale qui fournit un service numérique en santé dans un environnement de production à des utilisateurs.	L'éditeur du DPI qui met à disposition l'application aux professionnels de l'établissement.
Fournisseur d'identité (FI)	Entité qui crée et gère les identités électroniques de personnes physiques, délivre un moyen d'identification électronique et est responsable d'un ou plusieurs schémas d'identification électronique.	Pro Santé Connect peut jouer le rôle de fournisseur d'identité pour les professionnels de santé.
Fédérateur de fournisseurs d'identité	Service d'intermédiation entre les fournisseurs d'identité et les fournisseurs de service. Permet à un FS de disposer d'une solution unique d'identification tout en laissant le choix du FI à l'utilisateur.	France Connect est un fédérateur de fournisseurs d'identités.
Single Sign-On (SSO)	Mécanisme permettant à un utilisateur de ne s'authentifier qu'une fois pour accéder à plusieurs applications.	Le professionnel se connecte une seule fois le matin et accède ensuite au DPI, à la messagerie et à la pharmacie sans ressaisir ses identifiants.
eSSO (Enterprise SSO)	Mécanisme permettant la saisie automatique des mots de passe applicatifs à la place de l'utilisateur. Nécessite un agent logiciel sur le poste. Non-intrusif sur les applications existantes.	Agent SSO installé sur les postes du CHU qui remplit automatiquement les formulaires de connexion des applications métier.
WebSSO	Mécanisme permettant l'accès à plusieurs applications web dans un même navigateur avec une seule authentification. Les mécanismes de fédération (SAML, OpenID Connect) sont une approche standardisée du WebSSO.	Accès au portail patient, à la messagerie MSSanté et au DMP depuis le navigateur après une seule authentification Pro Santé Connect.

IE - HÔPITAL

Les réalités hospitalières nécessitent une lecture sectorielle

> Si le cadre réglementaire et la trajectoire IE s'appliquent à l'ensemble du secteur santé, le **contexte hospitalier** présente des spécificités majeures qui justifient une déclinaison opérationnelle dédiée.
>
> L'hôpital : c'est un environnement à haute criticité, fonctionnant en continu, avec une diversité de profils et d'usages que peu d'organisations connaissent.

Multiplicité des profils

Soignants titulaires, internes en rotation, intérimaires, prestataires externes, étudiants, chercheurs… Chaque catégorie a un cycle de vie différent, des droits spécifiques et des contraintes d'accès propres. Gérer cette diversité manuellement est source d'erreurs et de failles.

Organisation 24/7

Urgences, gardes de nuit, mobilité inter-services, postes partagés : l'accès aux systèmes doit être immédiat, fiable et adapté à des situations où chaque seconde compte. La sécurité ne peut jamais être un obstacle au soin.

SIH dense et hétérogène

DPI, imagerie, biologie, pharmacie, outils métier spécialisés… Le SI hospitalier est un écosystème complexe avec des dizaines d'applications, souvent de fournisseurs différents, avec des modes d'authentification disparates.

Risque de fragmentation

Sans cadre fédérateur, les établissements développent des solutions isolées, non harmonisées et difficiles à maintenir. Résultat : des silos, des incohérences et une dette technique croissante qui fragilise la posture de sécurité.

L'hôpital n'est pas une organisation comme les autres. La démarche HospiConnect donne un cadre pour prioriser les points à adresser, à charge pour chaque établissement de les mettre en œuvre au regard de ses propres contraintes sans jamais opposer sécurité et continuité des soins.

IE - HÔPITAL

HospiConnect : la bannière unifiée pour la mise en œuvre opérationnelle en établissement

> HospiConnect n'est **pas un nouveau cadre réglementaire**. C'est la réponse aux enjeux de sécurité opérationnelle spécifiquement conçue pour le secteur hospitalier. Son rôle : rendre mobilisable, pilotable et finançable le projet de transformation de la chaine de sécurisation de l'identification électronique en le mettant en cohérence et en le rendant lisible pour les équipes de terrain.

HospiConnect : accélérer la transformation des établissements sanitaires

MI - 2027 à FIN - 2028

- Une majorité d'ES ont déployé des Moyens d'Identification Electronique (MIE) sécurisés, permettant d'intégrer la consultation du DMP dans un DPI issu de la vague 2 du Ségur numérique, dans une trajectoire permettant leur généralisation à l'ensemble des utilisateurs du SIH
- Tous les professionnels disposent d'un MIE compatible avec Pro Santé Connect ou homologué en regard de la PGSSI-S et tous les services numériques en santé sont accessibles avec ce MIE, en limitant les contraintes d'authentifications multiples.

Une vision complète du projet

HospiConnect rassemble, dans une même lecture, l'ensemble des sujets à adresser pour sécuriser la chaîne d'identification électronique en établissement.
La démarche permet de visualiser le projet dans sa globalité, d'en comprendre les composantes et d'éviter une approche fragmentée.

Une trajectoire structurée pour agir

HospiConnect transforme le cadre en repères concrets pour conduire le projet : étapes, priorités, ressources mobilisables, livrables et jalons. Il aide les établissements à construire une trajectoire réaliste, progressive et adaptée à leur niveau de maturité.

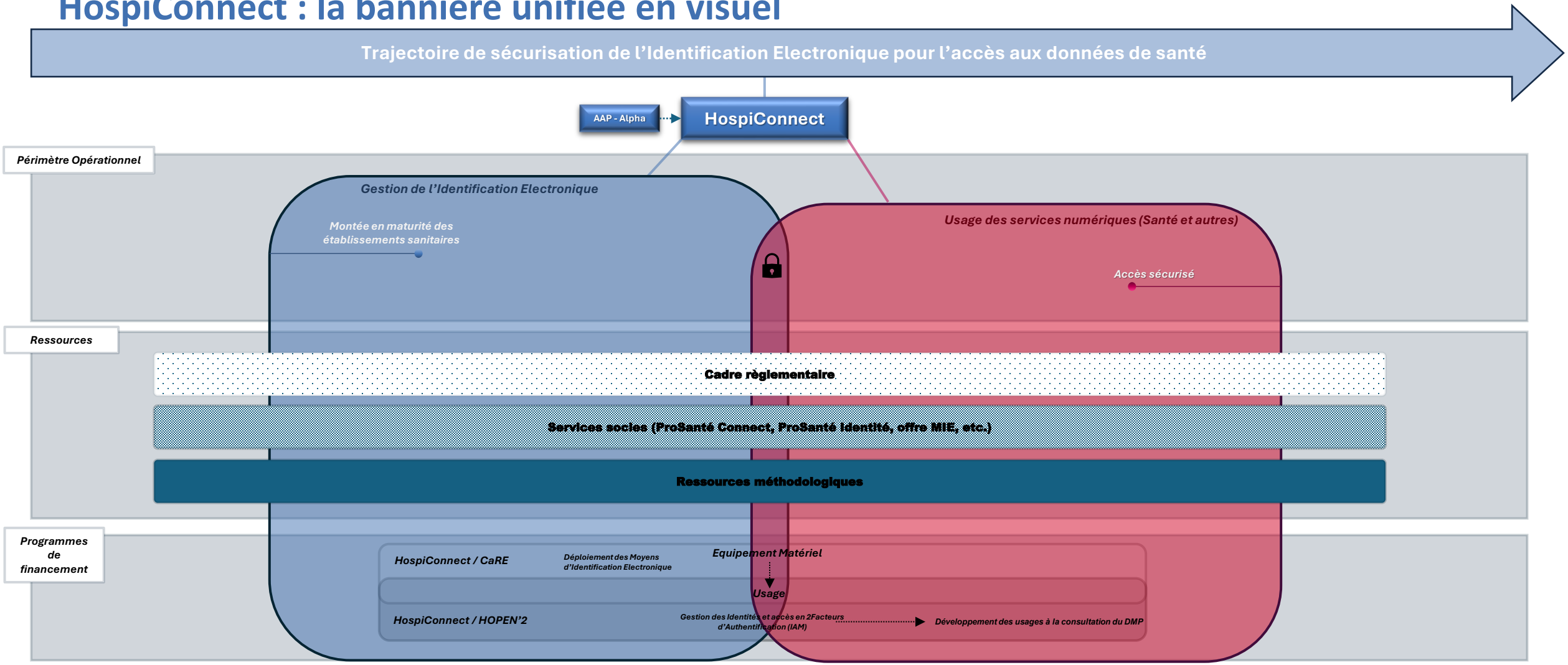
Des repères clairs pour piloter

HospiConnect met à disposition une lecture compréhensible et exploitable par les équipes projet, la DSI, les directions et les parties prenantes. Les enjeux sont clarifiés, les priorités rendues lisibles et les actions plus faciles à piloter dans le temps

💡 **HospiConnect ne crée pas un nouveau cadre : il rend le cadre lisible, actionnable et pilotable en établissement.** C'est un levier de transformation pour passer d'exigences dispersées à une démarche structurée, cohérente et opérationnelle.

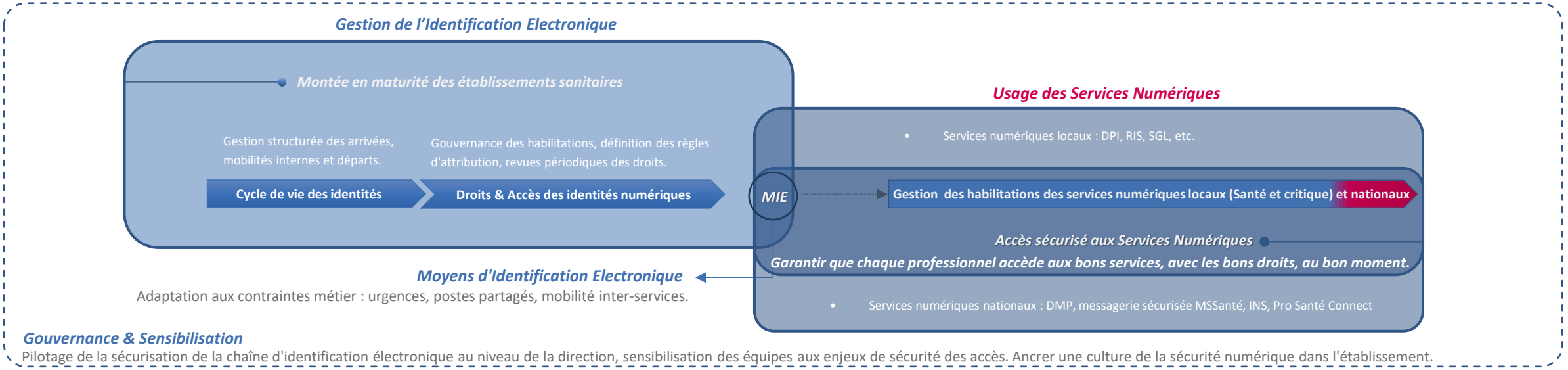
IE - HÔPITAL

HospiConnect : la bannière unifiée en visuel



Le périmètre HospiConnect : du cycle de vie à l'accès sécurisé aux services numériques

HospiConnect couvre l'ensemble du **parcours de gestion des identités et des accès** en établissement de santé. Il ne s'agit pas d'un outil unique ou d'une solution technique isolée, mais d'un périmètre fonctionnel complet qui adresse les cinq dimensions essentielles d'une gestion des accès maîtrisée. Chaque dimension est indissociable des autres : elles forment un tout cohérent.



Point clé : HospiConnect couvre le « bout en bout » pas seulement un outil ou une carte, mais l'ensemble de la chaîne identité - accès.

Webinaire dédié le 19/03 de 14h - 15h30

Agence du Numérique en Santé

HospiConnect - une identité numérique fiable et maîtrisée dans les services numériques en santé du secteur hospitalier

Episode #1 - Périmètre opérationnel

*** En rouge : gestion hors scope du périmètre opérationnel HospiConnect**

COMPOSANTES HOSPICONNECT

Services socles de l'ANS : s'appuyer sur les briques nationales

> L'ANS met à disposition un ensemble de **services socles** sur lesquels les établissements peuvent s'appuyer pour construire leur dispositif de gestion des identités et des accès. La démarche HospiConnect facilite articulation de ces briques dans le contexte spécifique de chaque établissement.

Services d'identité numérique

Référentiels d'identité des professionnels, outils de vérification.

Services d'authentification

Moyens d'authentification forte (Pro Santé Connect), mécanismes de fédération d'identité et de SSO.

Service d'immatriculation

RPPS, FINESS : les référentiels nationaux qui alimentent et fiabilisent les données d'identité locales.

La logique de convergence

L'enjeu n'est pas de remplacer les solutions locales, mais de les faire **converger** vers les standards nationaux pour garantir :

- **Cohérence** : les mêmes règles appliquées partout
- **Interopérabilité** : des systèmes qui se parlent
- **Pérennité** : des investissements qui durent

🔑 **Point clé :** Les services socles sont maintenus, documentés et mis à jour par l'ANS. Ils évoluent en fonction du cadre réglementaire et des retours terrain. L'établissement n'a pas à porter seul la charge de la conformité technique

Webinaire dédié le 24/03 de 14h - 15h30

Agence du Numérique en Santé

HospiConnect - une identité numérique fiable et maîtrisée dans les services numériques en santé du secteur h

Episode #2 - Les services socles de l'ANS

COMPOSANTES HOSPICONNECT

Référentiel d'identification électronique Version 2

> Définir les exigences applicables aux moyens d'identification électronique des acteurs des secteurs sanitaire et autres pour qu'une identité fiable accède aux bons services, au bon niveau de confiance.

Pilier de la PGSSI-S, le RIE est rendu opposable par arrêté ministériel le 28 mars 2022. La version 2, en attente de publication par arrêté, intégrera des mises à jour issues des remontées terrain des établissements, renforçant son applicabilité concrète. Elle s'appliquera aux secteurs sanitaire, médico-social et social.

Ce que le RIE impose

Répertoire d'identité fiable - Chaque professionnel doit être rattaché au RPPS (répertoire de référence national), garantissant une identité unique au niveau national, demain au niveau européen.

Moyen d'identification adapté - Chaque professionnel doit disposer d'un MIE adapté pour s'authentifier sur les services numériques en santé et prouver que la personne identifiée est bien celle qui se connecte.

Authentification renforcée obligatoire - Depuis le 1er janvier 2026, les MIE utilisés doivent faire intervenir une authentification à double facteur, par l'intermédiaire des MIE encadrés par la puissance publique (Pro Santé Connect) ou des MIE auto - homologués.

Ce que la v2 apportera

Remontées terrain intégrées - Les retours d'expérience des établissements auront été pris en compte pour clarifier les exigences et faciliter leur mise en œuvre opérationnelle.

📋 **Le RIE** détermine la trajectoire de sécurisation progressive de l'identification électronique des professionnels intervenant dans le système de santé. HospiConnect traduit ces exigences en feuille de route opérationnelle pour l'établissement.

📅 Webinaire dédié [à venir]

COMPOSANTES HOSPICONNECT

Un appui au plus près des établissements

> La transformation numérique se construit **au plus près des établissements**, avec des relais régionaux qui jouent un rôle essentiel de médiation, de coordination et d'accélération. Les ARS, les GRADeS et les équipes régionales d'appui constituent le maillage territorial indispensable à la réussite du programme HospiConnect.

Diffusion & mobilisation

Les relais régionaux assurent la diffusion auprès des établissements de leur territoire. Ils organisent des sessions d'information, des ateliers de sensibilisation et des temps d'échange pour faciliter l'appropriation du cadre et des ressources HospiConnect. Leur rôle est de **traduire le national en local**.

Partage de ressources & retours d'expérience

Les GRADeS et équipes d'appui facilitent le **partage entre pairs** : retours d'expérience de déploiement, bonnes pratiques, écueils à éviter, mutualisation d'outils et de compétences. Aucun établissement ne devrait se sentir seul face à la complexité du sujet.

Lien stratégie nationale ↔ réalité terrain

Les acteurs régionaux font remonter les réalités du terrain vers le niveau national et font redescendre les orientations stratégiques vers les établissements. Ce **double flux** est essentiel pour ajuster le programme aux besoins réels et accélérer l'appropriation locale.

🤝 **L'objectif :** accélérer l'appropriation et éviter l'isolement des établissements. La transformation se fait ensemble, pas seul.

COMPOSANTES HOSPICONNECT

Une transformation soutenue par des programmes de financement

> La mise en œuvre de la trajectoire HospiConnect représente un investissement significatif pour les établissements en temps, en compétences et en moyens. C'est pourquoi deux **programmes de financement nationaux** viennent soutenir et accélérer cette transformation. Ils ne se substituent pas à l'effort local, mais ils permettent d'amorcer, de structurer.

Volet matériel

🛡️ CaRE — Cybersécurité accélération et Résilience des Établissements

"le socle sécurité et matériel"

Le programme **CaRE** est le cadre opérationnel et financier national de cybersécurité des établissements. Dans le périmètre HospiConnect, il porte le financement du **socle matériel** nécessaire au renforcement de l'identification électronique des professionnels et au déploiement de l'authentification à deux facteurs. Plus largement, CaRE s'inscrit dans un plan d'action 2023-2027 structuré autour de quatre axes **gouvernance et résilience, ressources et mutualisation, sensibilisation, sécurité opérationnelle** avec plusieurs domaines ouverts, dont un guichet dédié **HospiConnect**.

Volet fonctionnel et organisationnel

🚀 HOP'EN2 — Hôpital Numérique ouvert sur son Environnement, phase 2

"la transformation organisationnelle et métier"

Le programme **HOP'EN2**, action majeure de la feuille de route 2023-2027, prend le relais de **HOP'EN** et **SUN-ES** pour accompagner la transformation numérique des établissements de santé. Dans sa phase 2026-2028, le dispositif **HospiConnect/HOP'EN2** est centré sur la **gestion des identités et des accès** ainsi que sur **l'accès en consultation au DMP**. Il finance les projets de transformation des pratiques et des organisations, avec des cibles progressives par année autour de deux objectifs : maîtriser la chaîne de gestion des identités et des accès au SIH, puis rendre effectif l'accès automatique au DMP pour les professionnels autorisés

HospiConnect s'appuie sur deux niveaux de soutien : CaRE pour équiper et sécuriser, **HOP'EN2** pour transformer et déployer.

Webinaire dédié le 26/03 à 16h

A RETENIR

Ce que HospiConnect met à disposition

> Au-delà du cadre et de la trajectoire, HospiConnect apporte un **outillage concret et opérationnel** pour accompagner les établissements à chaque étape de leur transformation. L'objectif est clair : vous donner un **chemin**, pas seulement des exigences. Voici ce que vous pouvez mobiliser dès maintenant.

📋 Un cadre lisible « hôpital »

Hospiconnect propose une lecture sectorielle, adaptée au contexte hospitalier, des exigences, référentiels, services socles et évolutions attendues. La démarche permet de rendre cet ensemble plus compréhensible, applicable et mobilisable par les établissements, afin d'identifier les sujets à adresser, de les prioriser et de construire une trajectoire de transformation progressive.

📖 Des ressources méthodologiques

La démarche consiste également à mettre à disposition des repères, supports et outils pour aider les établissements à cadrer, organiser et mettre en œuvre leur projet : ressources de compréhension, grilles de lecture, trames, exemples de démarches, points d'attention et éléments utiles pour construire une feuille de route adaptée à leur contexte.

📊 Un outillage de pilotage

Dans ce contexte, des indicateurs de maturité sont également proposés afin que les établissements puissent s'autoévaluer, suivre leur évolution et orienter leur progression. Ces outils permettent de mesurer objectivement les progrès, d'identifier les priorités et d'inscrire le projet dans une dynamique de suivi à long terme.

🤝 Une logique d'accompagnement

Hospiconnect repose sur une mobilisation nationale et en région pour accompagner le déploiement de la démarche au plus près du terrain. Cette dynamique permet d'aligner les repères, de relayer les ressources, de soutenir les établissements et de créer les conditions d'une mise en œuvre progressive et cohérente.

SYNTHESE

Synthèse & prochaines étapes

> Ce premier webinaire avait pour objectif de poser le décor : comprendre **pourquoi** HospiConnect existe, dans quel **contexte** il s'inscrit, et quelle **logique** il porte. Voici les trois messages essentiels à retenir.

1. Le cadre se renforce

Au niveau européen comme national, les exigences en matière de confiance numérique, de cybersécurité et de protection des données de santé s'intensifient. Ce mouvement est irréversible et concerne directement les établissements de santé.

2. La trajectoire IE est claire

L'objectif est limpide : une identité fiable, un accès fort à deux facteurs, une maîtrise des habilitations et une traçabilité démontrable. C'est la colonne vertébrale de la sécurité des accès en santé.

3. HospiConnect rend tout cela opérationnel

HospiConnect est la déclinaison « hôpital » : il met en cohérence cadre, briques, ressources et financement dans une bannière unifiée, lisible et actionnable pour les équipes terrain.

Prochaines étapes

Webinaire #1

HospiConnect#PérimètreOpérationnel
[19/03]

Ressources en ligne

Accédez aux guides et outils HospiConnect

https://sante-gouv-9827.slite.page/p/sVKcP-ZTcdZ_vH/Guide-pour-la-securisation-et-la-simplification-de-l-identification-electronique-des-professionnels-en-structure

Lien Communication E-Santé

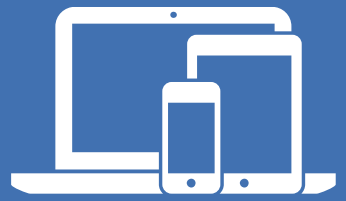
https://esante.gouv.fr/actualites/hospiconnect-une-identite-numerique-fiable-et-maitrisee-dans-les-services-numeriques-en-sante-du-secteur-hospitalier

Contact & questions

Mise en place FAQ **[à venir]**

AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici



esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'Agence du Numérique en Santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante