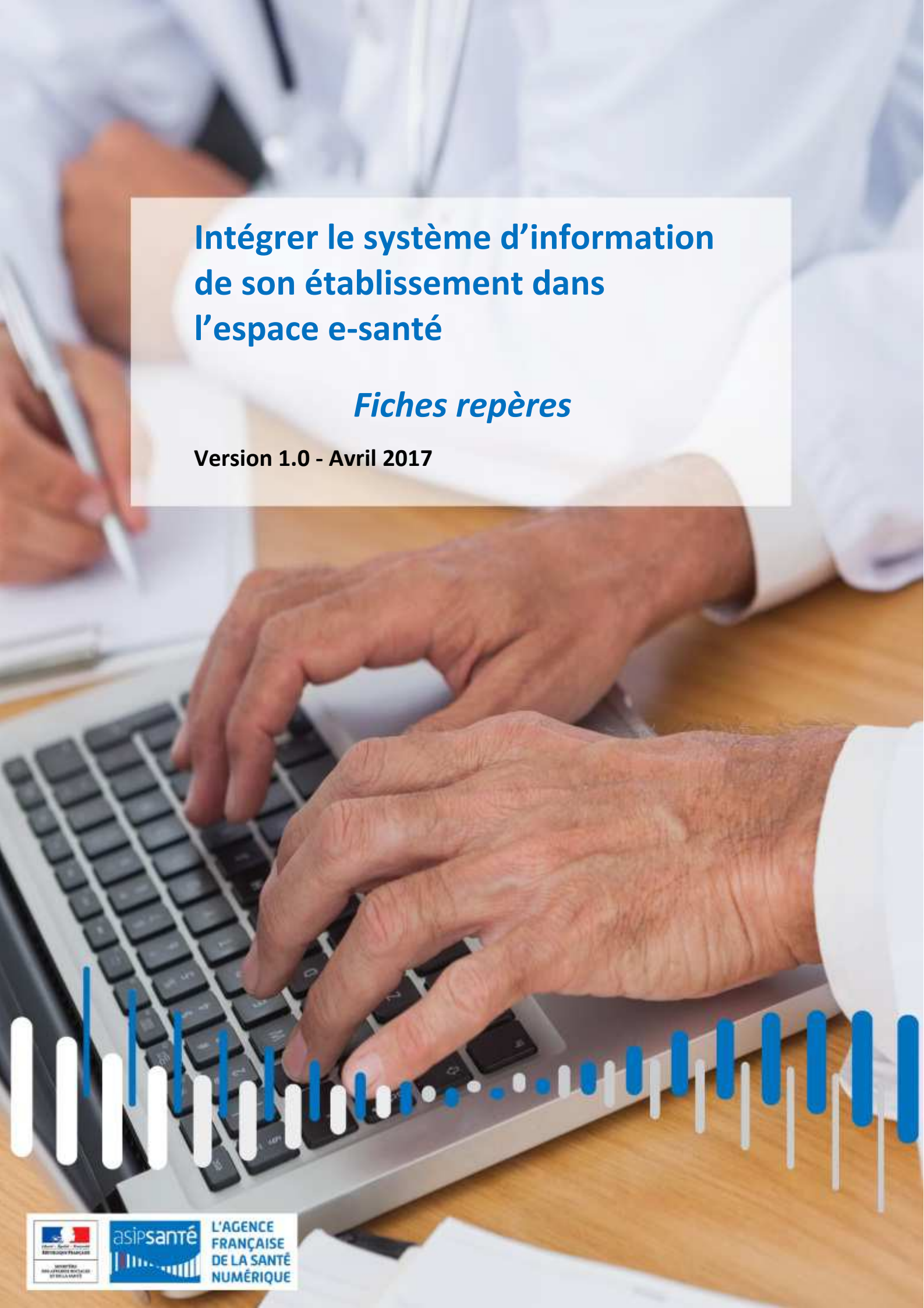


Intégrer le système d'information de son établissement dans l'espace e-santé

Fiches repères

Version 1.0 - Avril 2017

asipsanté
L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

OBJECTIFS DE CE LIVRET

Ce livret recense les thématiques sur lesquelles l'ASIP Santé peut appuyer les acteurs des établissements de santé et en particulier des groupements hospitaliers de territoire (GHT) lors de la construction, puis de la mise en œuvre de leur schéma directeur du système d'information (SI).

Il s'adresse aux équipes des établissements de santé, aux assistances à maîtrise d'ouvrage (**AMOA**) qui les aident à formaliser leur schéma directeur et aux maîtrises d'œuvre (**MOE**, éditeurs ou intégrateurs) qui les accompagnent dans la mise en œuvre. **Il a pour objectif de répondre, sous forme de fiches repères synthétiques, aux questions-clés** qui se poseront lors de la mise en œuvre du schéma directeur SI de l'établissement ou du GHT, sur les domaines d'expertise de l'ASIP Santé.

- Comment identifier les patients pris en charge par l'établissement et leurs partenaires ?
- Comment identifier les professionnels de santé intervenant en interne ou exerçant en dehors, en interaction avec l'établissement ?
- Comment sécuriser l'accès au système d'information de l'établissement ?
- Comment sécuriser l'hébergement des données de santé de l'établissement ?
- Comment favoriser l'interopérabilité entre les applications locales et les applications régionales et nationales de e-santé ?
- Quels outils utiliser pour échanger et partager les informations de santé avec l'ensemble des acteurs de santé participant à la prise en charge du patient dans le cadre de son parcours de soins ?
- …

CONSTRUIRE UN SCHEMA DIRECTEUR URBANISÉ DANS L'ECOSYSTEME E-SANTE

Le développement des parcours et des filières de soins implique la multiplication des échanges entre professionnels de santé et le partage croissant des données de santé.

Le développement du numérique en santé et les évolutions réglementaires (sur la notion d'équipe de soins notamment) facilitent le partage et l'échange d'informations entre les établissements de santé, les professionnels en ville et les secteurs médico-social et social.

Le schéma directeur SI doit ainsi prendre en compte deux composantes d'urbanisation :

- **L'urbanisation intra-établissement**, qui correspond, dans le cas particulier des GHT, à la trajectoire de convergence des SI GHT.
- **L'urbanisation extra-établissement**, qui correspond à l'articulation du SI de l'établissement (ou du GHT à terme) avec l'espace de la e-santé.

L'ASIP Santé, agence publique d'Etat composée de 130 collaborateurs, est chargée de favoriser le développement des systèmes d'information partagés et des technologies numériques dans les domaines de la santé et du secteur médico-social, afin de concourir au renforcement de l'efficacité des politiques de santé et à l'amélioration de la qualité, de la coordination et de l'efficience des soins.

POUR EN SAVOIR PLUS

- Site de l'ASIP Santé : ***esante.gouv.fr***

SOMMAIRE

Ce livret rassemble les fiches-repères en deux parties.

Partie 1 - Les référentiels :

Partie 2 - Les services :

Identifier le patient avec son identifiant national

FR
R1

UNE IDENTIFICATION COMMUNE DU PATIENT POUR FACILITER SA PRISE EN CHARGE

L'identification fiable des patients et des données les concernant est indispensable à la qualité de la prise en charge et à la sécurité des soins. En effet, des erreurs d'identification (doublons, collisions, documents mal attribués) peuvent avoir des conséquences graves dans la prise en charge du patient.

En conséquence, l'identifiant utilisé pour les patients en tant que porteurs de données de santé à caractère personnel doit être unique, univoque, pérenne et reconnu par tous les acteurs de santé.

L'IDENTIFIANT NATIONAL NIR PERMET CETTE IDENTIFICATION UNIQUE, UNIVOQUE ET PERENNE DU PATIENT.

La loi de modernisation de notre système de santé du 26 janvier 2016 consacre le NIR (Numéro d'Inscription au Répertoire national d'identification des personnes physiques) comme identifiant national de santé (INS). Le décret 2017-412 du 28 mars 2017 précise les modalités d'application.

Le NIR pourra être utilisé comme INS à compter de la publication du référentiel d'identification des usagers du secteur santé, médico-social et social, prévu avant le 31 mars 2018. Jusqu'alors, l'identifiant utilisé reste l'INS-C (l'identifiant national de santé calculé à partir des traits contenus dans la carte vitale du patient), créé pour le dossier médical partagé (DMP).

Le recours au NIR pour référencer les données de santé sera une obligation pour les acteurs qui concourent à la prise en charge sanitaire ou au suivi social et médico-social des personnes, à compter du 1er janvier 2020.

Toute personne assurée sociale est inscrite dans le **répertoire national d'identification des personnes physiques** (RNIPP) et dispose donc d'un NIR.

Le NIR est formé de 13 caractères : le sexe (1 chiffre), l'année de naissance (2 chiffres), le mois de naissance (2 chiffres) et le lieu de naissance (5 caractères). Les 3 chiffres suivants correspondent à un numéro d'ordre qui permet de distinguer les personnes nées au même lieu à la même période ; une clé de contrôle à 2 chiffres complète le NIR.

Le NIR est communément appelé « numéro de sécurité sociale ».

Cet identifiant doit être utilisé par l'ensemble des professionnels exerçant dans les établissements et les GHT ainsi que par les professionnels de santé extérieurs, quel que soit leur mode d'exercice (autres établissements, médecine de ville…), pour les patients qu'ils prennent en charge.

Les modalités de déploiement du NIR dans les systèmes d'information de santé sont à l'étude. Une étude, élaborée par l'ASIP Santé en complément du référentiel d'identification des usagers du secteur santé, médico-social et social, doit permettre de préciser ces modalités.

La solution privilégiée est l'ajout de deux champs complémentaires dans les systèmes d'information, permettant d'adjoindre à l'identifiant local (IPP dans les établissements de santé) **l'identifiant national** (le NIR accompagné de l'identifiant unique de l'autorité d'affectation du NIR).

Le NIR peut ainsi servir de trait d'identité et, à ce titre, faciliter le rapprochement entre les identifiants locaux des établissements, en particulier, lors de la mise en place d'une base patients commune dans le cadre des GHT.

Ce NIR sert également lors de l'appel des services nationaux comme le dossier médical partagé (DMP) ou le dossier pharmaceutique (DP).

COMMENT RECUPERER LE NIR (D'ORES ET DEJA DISPONIBLE POUR PLUS DE 75% DES FRANÇAIS) ?

Le NIR est d'ores et déjà disponible sur l'attestation de droits à l'assurance maladie du patient, pour les 66 millions de bénéficiaires de l'Assurance Maladie.

Le NIR est disponible dans la carte vitale du patient à partir du moment où le patient est l'ouvrant-droit (il s'agit de la majorité des cas soit 51 millions de personnes représentant 77% de la population).
Le NIR pourra être récupéré par le biais de téléservices de l'Assurance-Maladie, mis en œuvre au plus tard à partir du 31/12/2018, dans les cas où le NIR n'est pas disponible dans la carte vitale (il s'agit des ayants-droit du régime général, essentiellement les patients mineurs, inscrits dans la(les) carte(s) de leurs parents ou les adultes rattachés à un ouvrant-droit[1]).

Une minorité de patients n'auront jamais de NIR : il s'agit en particulier des patients étrangers sans AME (aide médicale d'état). Une règle d'identification de ces patients sera proposée dans le référentiel « identification des usagers» de la PGSSI-S.

Dans la majorité des cas (quand le patient correspond à l'assuré), **le NIR est d'ores et déjà une donnée collectée par les équipes administratives des établissements de santé**, généralement lors de l'accueil du patient, à des fins de facturation. Cette donnée existe donc déjà dans les applications de gestion administrative du patient (GAP) pour un certain nombre de patients.

Le NIR et l'identito-vigilance dans les établissements de santé.
Une fois le NIR du patient récupéré, celui-ci donne accès aux traits d'identité tels qu'enregistrés dans l'état civil. Il permettra donc de fiabiliser et d'harmoniser la saisie de l'identité du patient (noms et prénoms de naissance).

POUR EN SAVOIR PLUS

- Site de l'ASIP Santé : ***esante.gouv.fr/services***

[1]http://www.ameli.fr/assures/droits-et-demarches/la-protection-universelle-maladie.php

Construire les annuaires internes et de correspondants en s'appuyant sur les référentiels nationaux

FR R2

IDENTIFIER LES PROFESSIONNELS DE SANTE INTERVENANT EN INTERNE ET EN DEHORS, VIA UN ANNUAIRE CONVERGENT

Chaque établissement a besoin d'identifier :

- **l'ensemble des professionnels qui travaillent au sein d'un établissement** pour les rémunérer et faciliter l'attribution des droits d'accès physiques (parking, locaux,…) et logiques (accès au SI) ;
- **les acteurs de santé correspondants de l'établissement** pour permettre le partage et l'échange d'informations utiles à la coordination et à la continuité des soins.

La mise en place d'une gestion commune des données d'identification constitue la ressource clé du système d'information pour l'ensemble des processus de gestion des identités, des habilitations et des échanges.

Les enjeux sont multiples, car il faut pouvoir :

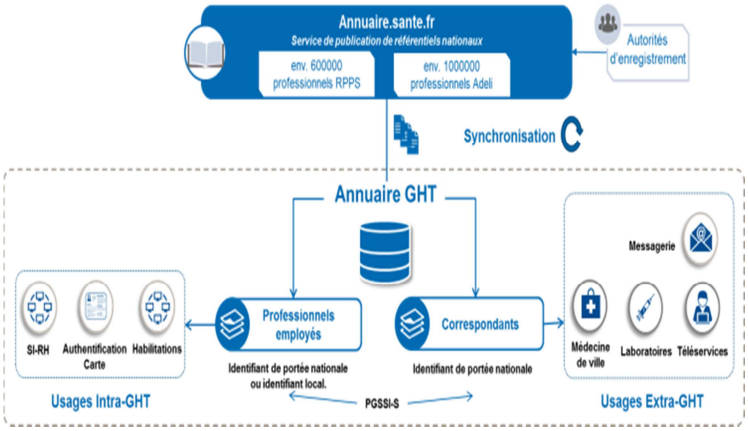
- avoir confiance dans l'exactitude des données d'identité ;
- minimiser les charges de peuplement et de maintenance de l'annuaire ;
- fédérer l'ensemble des applications.

COMMENT FIABILISER LES DONNEES D'IDENTIFICATION EN LES SYNCHRONISANT AUX REFERENTIELS NATIONAUX ?

L'ASIP Santé met en œuvre une plateforme de publication des données d'identification des professionnels de santé contenues dans les référentiels nationaux RPPS[2] et Adeli : annuaire.sante.fr.

Les données d'identification portent principalement sur l'identité du professionnel, ses données professionnelles (diplôme, profession, spécialité), ses coordonnées de correspondance (postale et messagerie sécurisée), son lieu d'exercice.

Dès à présent, tout établissement peut récupérer ces données pour alimenter quotidiennement ses annuaires, pour gérer l'identification de ses professionnels de santé ou pour faciliter la correspondance avec l'extérieur.



Exemple de schéma d'intégration de l'annuaire santé au sein d'un GHT.

Ces données couvrent l'ensemble des professionnels de santé :

- médecins, sages-femmes, pharmaciens, chirurgiens-dentistes et masseurs-kinésithérapeutes, enregistrés dans le RPPS.
- les autres professions de santé (infirmiers…), enregistrées dans le référentiel Adeli (dans l'attente que ces professions soient intégrées dans le RPPS).

[2] Répertoire partagé des professionnels de santé

Elles sont opposables car enregistrées et certifiées par les autorités concernées (DRESS pour Adeli, Ordres, Service Santé des Armées et INSEE pour le RPPS). Elles tiennent lieu de pièces justificatives.

L'utilisation des données des référentiels nationaux permet de :

- disposer de l'identifiant national des professionnels ;
- vérifier l'identité et les compétences des professionnels sans requérir de justificatifs ;
- réduire les charges de collectes et de mises à jour des données dans l'annuaire interne.

L'ASIP SANTE ACCOMPAGNE LES ETABLISSEMENTS ET LES GHT

✓ **Consolider les annuaires existants :** aide au rapprochement des identités.

L'ASIP Santé met à disposition des établissements un outillage et une méthodologie pour réaliser le rapprochement de l'annuaire local aux référentiels nationaux.
Cet accompagnement permet notamment, dans le cadre des GHT, de faciliter le peuplement initial de l'annuaire, en confiant à l'ASIP Santé les tâches de rapprochement. Le GHT dispose ainsi rapidement d'un annuaire consolidé, basé sur l'identifiant national RPPS/Adeli, dont les mises à jour sont facilement automatisables.

Cette démarche de rapprochement a été engagée en 2016 avec une trentaine d'établissements pour mettre à jour les données des prescripteurs dans le RPPS dans le cadre du suivi des prescriptions exécutées en ville.

✓ **Mettre en place la synchronisation :** automatiser les mises-à-jour.

La mise à jour des données d'annuaire de l'établissement est automatisable. L'ASIP Santé assiste à trois niveaux les acteurs souhaitant mettre en place les interfaces annuaire.sante.fr :

- mise à disposition de la documentation des interfaces ;
- accompagnement à la mise en œuvre technique ;
- assistance aux porteurs de projets dans l'utilisation des données.

✓ **Identifier l'ensemble des professionnels de l'établissement :** recommandations contenues dans le modèle d'identification des acteurs du secteur santé[3].

Au-delà des règles définies dans le référentiel d'identification des acteurs sanitaires et médico-sociaux de la PGSSI-S, l'ASIP Santé publie un socle commun de bonnes pratiques et de règles homogènes facilitant la mise en œuvre d'un annuaire des professionnels.

Ce modèle n'impose pas d'identifiant unique mais souligne l'importance de pouvoir maintenir dans le temps les liens entre les identifiants internes au système d'information et l'identifiant national du professionnel.

POUR EN SAVOIR PLUS

- Site de l'ASIP Santé : ***esante.gouv.fr/services***

[3] Ce document s'inscrit dans le corpus documentaire du cadre d'urbanisation sectoriel (santé), publication en cours par l'ASIP Santé

Sécuriser l'accès aux applications de santé en authentifiant les professionnels

FR
R3

AUTHENTIFIER LE PROFESSIONNEL QUI ACCEDE AUX SI DE SANTE

Le Référentiel Général de Sécurité (RGS) définit l'authentification dans les termes suivants : « L'authentification a pour but de vérifier l'identité dont se réclame une personne ou une machine (s'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité). »

L'authentification permet donc de sécuriser l'accès aux systèmes d'information utilisés par les professionnels, et tout particulièrement l'accès aux données sensibles telles que les informations de santé concernant le patient :

- en accordant un accès aux systèmes aux seules personnes autorisées ;
- en différenciant les possibilités d'accès aux services et aux données de santé en fonction des droits attachés à l'identité des utilisateurs ;
- en permettant d'imputer les actions à leur auteur.

Dans le cadre des établissements, il s'agit à la fois :

- De sécuriser, pour les professionnels travaillant dans les établissements, l'accès aux applications métiers des établissements (et au futur SI convergent dans le cas des GHT) ainsi que l'accès aux SI externes (DMP, plateforme de télémédecine…) que les professionnels sont amenés à utiliser de plus en plus.
- De sécuriser, pour les professionnels de santé hors de l'établissement (médecine de ville, professionnel accédant depuis son domicile…), l'accès au SI.
- De sécuriser l'accès des fournisseurs accédant au SI et donc aux données de santé (télémaintenance des équipements biomédicaux…).

DANS LE RESPECT DU REFERENTIEL D'AUTHENTIFICATION DE LA PGSSI-S

La politique générale de sécurité des systèmes d'information en santé (PGSSI-S) **publie le référentiel d'authentification des acteurs de santé des domaines sanitaire, médico-social et social**. **Ce référentiel,** bientôt opposable, guide les acteurs de santé dans le **choix des dispositifs d'authentification à mettre en œuvre** pour la protection des données de santé des patients.

Une révision du référentiel d'authentification de 2014 est en cours, afin de mieux faire ressortir les paliers d'authentification minimum requis selon :

- **Le niveau d'exposition des données de l'application**, en tenant compte des critères suivants :
  - caractéristique du réseau sur lequel est déployée l'application (réseau public ? réseau interne non cloisonné ?) ;
  - caractéristique de la zone physique dans laquelle se situe le terminal d'accès (zone physique ouverte au public sans contrôle d'accès ?) ;
  - caractéristique du terminal dédié ou mutualisé entre plusieurs utilisateurs.

- **Les liens contractuels** entre le responsable de traitement et l'utilisateur bénéficiant du dispositif d'authentification.

Le référentiel conserve la distinction entre l'authentification **privée** et l'authentification **publique** du professionnel, ainsi que la dissociation entre l'authentification **directe** du professionnel à une application et l'authentification **indirecte** (ou déléguée) via une **personne morale**.

Le niveau de confiance des différents dispositifs d'authentification susceptibles d'être mis en œuvre reste précisé selon trois paliers.

- Le palier 1 (minimum) est une **authentification simple** qui repose sur un seul facteur (par exemple un utilisateur qui indique son mot de passe). Ce palier ne s'applique que dans un contexte d'authentification privée.

- Le palier 3 (maximum) comprend des dispositifs **d'authentification forte**, combinant plusieurs facteurs différents. On y trouve par exemple la carte CPS qui permet de combiner « la carte à puce » détenue par le porteur (« ce qu'il possède ») et le code associé (« ce qu'il sait »).

La carte CPS.
La carte CPS est délivrée gratuitement par l'ASIP Santé. Un million de cartes de la famille CPS sont aujourd'hui en circulation. Intégrant nativement **l'identification nationale** du professionnel de santé et contenant des **certificats d'authentification et de signature**, elle permet une authentification directe du professionnel de santé auprès des applications métiers de l'établissement et des télé-services régionaux et nationaux. **Sa fonctionnalité « sans contact »** facilite son usage en situation de mobilité. La CPS est un **titre fondateur** permettant la mise en place de dispositifs d'**authentification alternatifs** (ex : enrôlement d'un terminal par carte CPS).

Plus de 60 établissements ont généralisé l'utilisation des cartes de la famille CPS, à la fois pour sécuriser l'accès aux systèmes d'information, mais également pour sécuriser les accès physiques (locaux, parking…) et parfois la personnalisent avec la photo du porteur.

COMMENT METTRE EN ŒUVRE UN DISPOSITIF D'AUTHENTIFICATION ADAPTE ?

La réalisation d'une analyse des risques en matière de sécurité du SI est obligatoire avant toute mise en œuvre d'un système d'information de santé.
Elle est effectuée par le responsable de traitement de l'établissement pour les applications locales ou par le(s) responsable(s) de traitement du (des) SI convergent(s) du GHT pour les applications du GHT, et par les responsables de traitement des télé-services nationaux et régionaux.

Elle facilite l'identification du palier minimum à mettre en œuvre pour sécuriser l'accès à l'application tel que décrit dans le référentiel d'authentification de la PGSSI-S, puis l**e choix des dispositifs d'authentification respectant ces exigences de sécurité et tenant compte des usages et de l'existant.**

Dans le cas particulier du GHT, le choix du mode d'authentification est complexifié par le fait que le GHT n'est pas une personne morale.

POUR EN SAVOIR PLUS

- PGSSI-S : ***esante.gouv.fr/services***
- Produits de certification délivrés par l'ASIP Santé : ***esante.gouv.fr/services***

Plus spécifiquement, consignes relatives aux mots de passe :

- ANSSI : ***www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf***
- CNIL : ***www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires***

Sécuriser le système d'information selon les normes en vigueur

FR
R4

DES BESOINS ACCRUS DE PROTECTION DES DONNEES DE SANTE

Le besoin croissant de coordination nécessite d'ouvrir davantage le SI hospitalier, pour permettre l'échange et le partage d'informations de santé entre les professionnels impliqués dans la prise en charge des patients (qu'ils soient du même établissement, du même GHT ou extérieurs).

L'évolution des pratiques nécessite de faciliter la mobilité des professionnels amenés à exercer sur plusieurs sites, notamment dans le cadre des GHT.

Favoriser l'ouverture du SI ainsi que la mobilité des utilisateurs implique cependant une réflexion accrue sur la sécurisation du SI. De nombreuses questions se posent, notamment :

- Quel identifiant choisir pour les acteurs professionnels ?
- Quels dispositifs d'authentification choisir pour sécuriser l'accès au SI et aux données de santé ?
- Comment gérer la traçabilité des accès au SI et aux données de santé ?
- Comment encadrer l'utilisation des tablettes dans les établissements ?
- Quelles sont les bonnes pratiques de sauvegarde ?

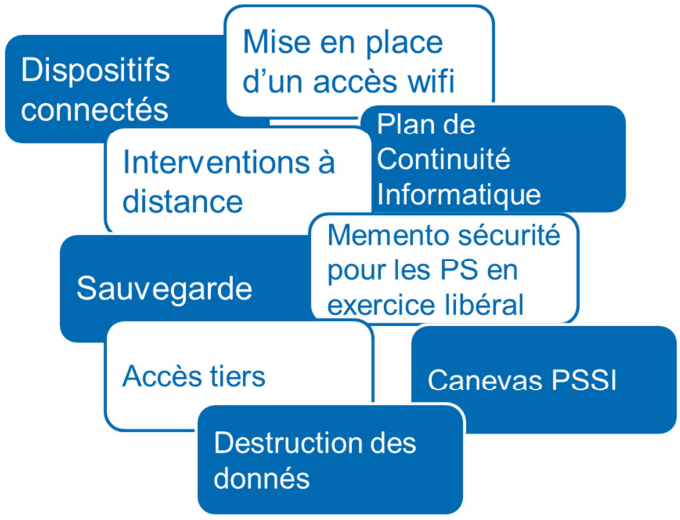
La politique générale de sécurité des systèmes d'information de santé (PGSSI-S) a pour objectif d'apporter des éléments de réponse à toutes ces questions.

LA PGSSI-S, UN CADRE POUR LA PROTECTION DES DONNEES DE SANTE

La PGSSI-S, établie sur le fondement de l'article L. 1110-4-1 du code de la santé publique**, définit les exigences et les recommandations liées à la protection des données de santé à caractère personnel**, dans le respect des droits du patient, dans des contraintes opérationnelles et économiques acceptables pour l'ensemble des acteurs des secteurs sanitaire, médico-social et social.

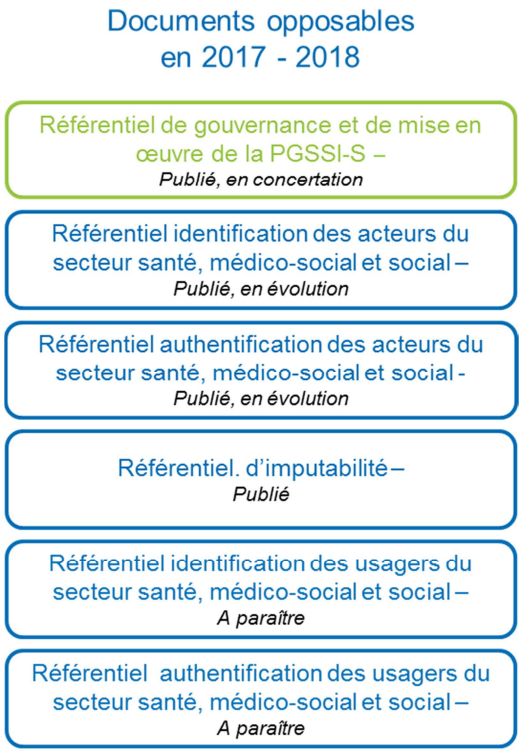
La PGSSI-S est un corpus documentaire composé de **guides et de référentiels à vocation opposable :**

Guides (liste non exhaustive)



Le guide d'élaboration et de mise en œuvre d'une PSSI apporte une aide à l'élaboration de la politique de sécurité du système d'information et à la mise en œuvre du plan d'actions associé.

Référentiels opposables



Les référentiels présentent différents niveaux d'exigences, appelés « paliers » :

Ces paliers techniques dépendent de la **maturité de l'établissement** et du **contexte d'usage**.
Ils comprennent :

- **un palier minimal** (palier 1) déjà opérationnel ou rapide à atteindre comportant les exigences de sécurité indiscutables,
- **un palier cible** (palier dont le numéro est le plus élevé) et paliers intermédiaires permettant de bâtir des trajectoires d'évolution et de satisfaire des objectifs de sécurité intermédiaires.

Ces paliers permettent de définir le niveau de sécurité cohérent avec les cas d'usage et les risques identifiés par l'établissement de santé.

L'ASIP SANTE AGIT POUR RENFORCER LA SECURITE DES SI DE SANTE

Outre le fait de gérer la sécurité des infrastructures[4] dont elle a responsabilité, l'ASIP Santé contribue à renforcer la sécurité des systèmes de santé à plusieurs titres :

- L'ASIP Santé **élabore les référentiels et guides de la PGSSI-S**, sous la responsabilité de la Délégation à la stratégie des systèmes d'information de santé (DSSIS) et en concertation avec les acteurs parties prenantes du domaine sanitaire, médico-social et social. La PGSSI-S est régulièrement actualisée avec le cadre juridique national (code de la santé publique, loi informatique et libertés…) et européen (GDPR, NIS, eIDAS…).
- L'ASIP Santé gère **la chaine de confiance permettant d'identifier puis d'authentifier les acteurs de santé**, depuis leur enregistrement par les autorités d'enregistrement nationales (ordres, ARS, service de santé des armées…) jusqu'à la délivrance de certificats électroniques assurée par l'ASIP santé pour sécuriser l'échange et le partage de données de santé.
- Les travaux menés pour favoriser l'interopérabilité entre les SI de santé contribuent à la normalisation des échanges, gage de confiance.
- A partir d'octobre 2017[5], l'ASIP Santé, en collaboration avec le HFDS et les services de la DGS, sera chargée **d'analyser les incidents graves et significatifs de sécurité** remontés par les établissements de santé, laboratoires de biologie médicale et centres de radiothérapie, et **d'apporter un appui aux acteurs.**

POUR EN SAVOIR PLUS

- Site de l'ASIP Santé : ***esante.gouv.fr/pgssi-s***

[4] L'ASIP Santé assure la maitrise d'ouvrage de nombreux systèmes d'information : RPPS, système CPS, MSSanté, etc.
[5] Nouvelle activité de l'ASIP Santé suite à la parution du décret 2016-1214 du 12/09/2016 relatif aux conditions de signalement des incidents graves de sécurité (application de l'article 110 de la loi n 2016-41 du 26 janvier 2016 de modernisation de notre système de santé)

Héberger les données de santé à caractère personnel

FR
R5

LE CADRE JURIDIQUE DE L'HEBERGEMENT DE DONNEES DE SANTE

Tout responsable de traitement doit s'assurer de mettre en œuvre (lui-même ou en ayant recourt à des sous-traitants) **les mesures de sécurité adaptées à la sensibilité des données** (cf. article 34 de la loi « Informatique et Libertés).

Ces mesures concernent notamment la conservation des données de santé, qui fait l'objet d'un encadrement spécifique défini par l'article L.1111-8 du code de la santé publique[6].
Cet article a pour finalité d'organiser et d'encadrer le dépôt, la conservation et la restitution des données de santé à caractère personnel dans des conditions propres à garantir leur confidentialité et leur sécurité :

- toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte d'un tiers, doit être agréée à cet effet ;
- l'hébergement exige une information claire et préalable de la personne concernée par les données de santé hébergées et une possibilité pour celle-ci de s'y opposer pour motif légitime.

LA PROCEDURE ACTUELLE[7]

Le décret n° 2006-6 du 4 janvier 2006[8] est venu préciser l'article L.1111-8. Il définit le **déroulement de la procédure d'agrément** pour l'hébergement de données de santé sur support informatique **et les exigences à respecter** :

- le décret fixe le contenu du dossier de demande d'agrément. Sont ainsi évalués la capacité financière du candidat, le type de prestation proposée, le niveau de sécurité et les conditions du respect des principes de la protection des données personnelles et des droits des personnes.
- l'agrément est délivré par type de prestation, pour une durée de trois ans par le ministre chargé de la Santé après avis de la Commission nationale de l'informatique et des libertés (CNIL) et du comité d'agrément des hébergeurs (CAH - organe consultatif créé par le décret précité). Si l'hébergeur agréé souhaite poursuivre son activité d'hébergement au-delà des trois ans initiaux, il doit effectuer une demande de renouvellement d'agrément qui sera instruite comme la demande initiale.

[6] modifié par la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[7] Voir infra point sur le remplacement de la procédure d'agrément par une procédure de certification.

[8] Décret codifié aux articles R.1111-9 à R.1111-15-1 du code de la santé publique.

L'EVOLUTION DE LA PROCEDURE D'AGREMENT VERS UNE PROCEDURE DE CERTIFICATION

L'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel - qui entrera en vigueur à une date fixée par décret et au plus tard le 1er janvier 2019 – **remplace l'actuelle procédure d'agrément pour l'hébergement de données de santé à caractère personnel sur support électronique par une évaluation de conformité à un référentiel de certification**, délivrée par un organisme certificateur accrédité par le COFRAC (ou équivalent au niveau européen) et choisi par l'hébergeur.

La procédure de certification se fonde sur le processus standard de type système de management décrit dans la norme ISO/CEI 17021 :

- l'hébergeur choisit un organisme certificateur accrédité par le COFRAC (ou équivalent au niveau européen) ;
- le cas échéant, l'organisme certificateur vérifie l'équivalence des éventuelles certifications ISO 27001 ou ISO 20000 déjà obtenues par l'hébergeur ;
- un audit en deux étapes conformes aux normes en vigueur est alors effectué : un audit documentaire (pouvant être réalisé sur le site d'hébergement), puis un audit sur site.

La future procédure de certification, ainsi que sa date de mise en œuvre seront définies par décret en Conseil d'Etat.

Le référentiel de certification

Il est basé sur des normes internationales existantes :

- les exigences de la norme ISO 27001 « système de gestion de la sécurité des systèmes d'information » ;
- des exigences de la norme ISO 20000 « système de gestion de la qualité des services» ;
- des exigences de la norme ISO 27017 « code de pratique pour les contrôles de sécurité de l'information pour les services du nuage »,
- des exigences de la norme ISO 27018 « protection des données à caractère personnel » ;
- et des exigences spécifiques à l'hébergement de données de santé.

POUR EN SAVOIR PLUS

- Site de l'ASIP Santé : ***esante.gouv.fr/services***

Favoriser l'interopérabilité des différents systèmes d'information

FR
R6

UN CADRE D'INTEROPERABILITE POUR CREER LES CONDITIONS DE L'ESSOR DE LA E-SANTE

La prise en charge continue et coordonnée du patient par l'ensemble des acteurs en santé (sanitaire, médico-social et social) **implique que les systèmes d'information de ces acteurs soient en capacité d'interagir aisément entre eux**, de manière interopérable (c'est-à-dire en utilisant le même langage) et sécurisée.

Pour pérenniser les investissements tant du côté des éditeurs de logiciels que de leurs clients, les pouvoirs publics ont favorisé la mise en place d'un cadre d'interopérabilité des systèmes d'information en santé (CI-SIS) s'appuyant sur des normes et standards internationaux matures et stables et tenant compte des contextes d'usage.

LE CI-SIS, UNE INTEROPERABILITE A LA FOIS SEMANTIQUE ET TECHNIQUE

Construit en concertation avec les représentants des professionnels de santé et les éditeurs des systèmes d'information de santé, **le CI-SIS fixe les règles d'une informatique de santé communicante en France.** Il couvre :

- **l'interopérabilité technique**, qui porte sur le transport des flux et sur les services garantissant l'échange et le partage des données de santé dans le respect des exigences de sécurité et de confidentialité des données personnelles de santé.
- **l'interopérabilité des contenus métiers**, qui permet l'échange et le partage des données de santé et leur compréhension par les systèmes d'information en s'appuyant sur un langage commun.

A titre d'exemple, le CI-SIS contient les spécifications de la synthèse médicale du patient (VSM) (produite un médecin via son logiciel métier), du dossier de liaison d'urgence (DLU) du résident (produit par le médecin coordinateur via le logiciel utilisé en EHPAD) ou de la lettre de liaison (la lettre de liaison d'entrée en hospitalisation étant produite par les médecins de ville dans leur logiciel métier et celle de sortie par les professionnels en établissement de santé, via le SIH).

Les spécifications d'interopérabilité du CI-SIS reposent sur l'identification et la compréhension partagée de concepts métiers (ou objets) correspondant aux informations manipulées par les systèmes d'information de santé (telles les informations relatives au professionnel de santé) qui sont catalogués dans le **Modèle des objets de santé (MOS)**.

Publié dans sa première version en 2009 puis régulièrement mis à jour, le CI-SIS a principalement permis de couvrir les cas d'usage liés au partage et à l'échange de documents de santé dans le cadre de la coordination des soins, favorisant ainsi le déploiement du DMP et des messageries sécurisées de santé (MSSanté).

De facto, les éditeurs disposant d'applications « DMP compatibles » ont développé des interfaces conformes au CI-SIS pour pouvoir s'interfacer avec le DMP, dans le respect de la démarche d'homologation à la « DMP compatibilité » et du dossier de spécifications fonctionnelles et techniques des interfaces DMP des logiciels de professionnels de santé.

Le CI-SIS s'ouvre désormais à de nouveaux cas d'usage pour lesquels un besoin d'interopérabilité entre systèmes se fait sentir.

A titre d'exemple, le CI-SIS s'enrichit de spécifications relatives à la gestion d'un agenda partagé et à la notification d'évènements (permettant par exemple d'informer les professionnels de santé en ville que leur patient est hospitalisé).

COMMENT FAIRE REMONTER LES BESOINS D'INTEROPERABILITE ?

Les établissements, entre autres acteurs, peuvent être confrontés :

- d'une part, à un **besoin d'interopérabilité entre les briques applicatives qui composent le** SI (et notamment le SI convergent dans le cas des GHT),
- **d'autre part, à un besoin d'interopérabilité avec les partenaires extérieurs à l'établissement ou au groupement,**

et souhaiter que ce besoin puisse donner lieu à un enrichissement du CI-SIS.

L'établissement, en associant s'il le souhaite sa maîtrise d'œuvre, peut :

- dans le cas des GHT, préalablement **utiliser le guichet *www.si-ght.fr* pour échanger avec les autres GHT sur son (ses) besoin(s) d'interopérabilité**, et voir si d'autres GHT sont également concernés et intéressés à porter collectivement cette demande,
- **remplir et transmettre à l'ASIP Santé le formulaire d'expression de besoins d'interopérabilité** (qui contient notamment la description des cas d'usage métiers effectuée par les établissements) en suivant la démarche décrite dans : *esante.gouv.fr/services/referentiels/ci-sis/demarche-elaboration.* Ce formulaire standard est destiné à tout acteur qui souhaite remonter un besoin d'interopérabilité.

La demande est ensuite étudiée par les experts de l'ASIP Santé en charge du CI-SIS :

- **Analyse des besoins** d'un point de vue fonctionnel et technique, pour vérifier s'ils sont à prendre en compte pour faire évoluer le CI-SIS ou s'ils doivent être traités d'une autre manière.
- **Après validation par le comité d'instruction** du degré de priorisation de ces besoins (au regard des autres demandes reçues), évolution du CI-SIS : **choix de la norme ou du standard** permettant de couvrir ces besoins, **rédaction des spécifications d'interopérabilité**, **concertation publique** et **intégration finale dans le CI-SIS**.

POUR EN SAVOIR PLUS

- Présentation du CI-SIS: ***esante.gouv.fr/services***
- Le modèle des objets de santé (MOS) et les nomenclatures associées : ***esante.gouv.fr/services***

Partager et échanger les données de santé

FR R7

La possibilité d'échanger et de partager des données de santé au-delà des murs de l'hôpital et entre des professionnels ne relevant pas tous du secteur sanitaire a été consacrée par la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, en modifiant les règles fixées à l'article L. 1110-4 du code de la santé publique et en créant l'article L. 1110-12 du même code, relatif à l'équipe de soins définie pour la première fois.

Le législateur a ainsi tenu compte des nouvelles modalités de prise en charge des personnes, dont les GHT font partie.

LES PRINCIPES GENERAUX ET CONDITIONS PARTICULIERES A RESPECTER EN CAS D'ECHANGE OU DE PARTAGE DE DONNEES DE SANTE

Le principe général est, et reste l'obligation de respecter le secret professionnel.

La loi permet d'y déroger pour permettre l'échange et le partage de certaines données de santé à caractère personnel dans de nouvelles conditions :

- l'échange et le partage ne sont possibles qu'entre professionnels participant à la prise en charge d'une même personne ;
- seules les informations strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou au suivi médico-social et social de la personne peuvent être échangées ou partagées.
- l'échange ou le partage d'informations entre professionnels faisant partie de la même équipe de soins supposent d'informer le patient au préalable (sans recueil du consentement) : le patient dispose d'un droit d'opposition ;
- le partage d'informations entre professionnels ne faisant pas partie de l'équipe de soins nécessite de recueillir le consentement exprès du patient.

LA NOTION D'EQUIPE DE SOINS DANS LE CAS PARTICULIER DU GHT

La notion d'équipe de soins, auparavant réservée aux professionnels exerçant au sein d'un même établissement de santé est étendue notamment au cas du GHT.

La notion d'équipe de soins est une notion clé pour les GHT : en effet, le projet médical partagé du GHT prévoit la mise en place d'équipes médicales communes et institue de ce fait de nouvelles définitions d'équipes de soins.

Les GHT doivent donc s'approprier la notion d'équipe de soins, à la fois pour :

- déterminer et identifier les modalités d'échange ou de partage de données de santé et garantir le respect des droits des patients ;
- mettre en place les mécanismes adéquats de protection des données de santé des patients pris en charge au sein du GHT.

Les professionnels qui exercent au sein des GHT sont réputés constituer une équipe de soins à condition de participer directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes.

Les informations de santé sont réputées confiées à l'ensemble de l'équipe de soins.

LES MESURES DE PROTECTION DES DONNEES DE SANTE

La déontologie des professionnels de santé est la première mesure de protection des données de santé.
En en cas d'accès illicite aux données de santé, c'est-à-dire, sans motif de soins, les risques encourus relèvent du pénal (15 000 euros d'amende et un an d'emprisonnement).

Au-delà, au sein des établissements, des mesures organisationnelles et techniques doivent être mises en place pour veiller à la sécurité des données de santé traitée dans le cadre des activités de soins de l'établissement ou du GHT.

Certaines de ces mesures permettront de **faciliter et contribuer au respect des conditions légales d'échange et de partage des données de santé** telles que la signature de la charte d'accès aux données de santé, la définition de grilles d'habilitation par profil, la mise en œuvre de blocages SI ciblés…

Au-delà de ces mesures de contrôle *a priori*, des contrôles aléatoires *a posteriori* d'accès aux dossiers peuvent être réalisés.

L'accès aux données de santé
L'accès aux données de santé est à distinguer de l'accès au système d'information: l'accès aux données de santé peut se faire par la création de comptes utilisateurs dans le SI ; mais il peut y avoir accès aux données de santé sans accès au système d'information (par exemple, remise d'un support de sauvegarde comportant les données de santé extraites du SI).
Autre exemple, le fait de réceptionner sous format papier un extrait d'une base de données de santé est considéré comme un accès aux données de santé.
La PGSSI-S éclaire les acteurs sur les modalités de protection des données de santé *(cf. fiche R4).*

En outre, les systèmes d'information utilisés doivent obligatoirement faire l'objet de mesures de sécurité adaptées à la sensibilité des données de santé.

Ces mesures de protection doivent être étudiées par l'établissement, en impliquant notamment les représentants du corps médical, des soignants et de la DSI, qui doivent réaliser leur propre analyse de risques.

POUR EN SAVOIR PLUS

- Site ASIP Santé : ***esante.gouv.fr/services***

Accéder à l'offre de soins via le ROR pour orienter le patient

FR R8

UN REPERTOIRE AU SERVICE DU PARCOURS DE SANTE DE LA PERSONNE

Le ROR, répertoire opérationnel des ressources, est positionné par les acteurs institutionnels comme le référentiel de la description opérationnelle de l'offre de santé. Les régions sont responsables du déploiement et du peuplement du ROR de leur région sur l'ensemble des champs d'activité du sanitaire et du médico-social.

Le ROR est un composant essentiel en matière de SI de santé pour faciliter l'orientation du patient, et ainsi éviter les ruptures dans son parcours de santé et lui garantir l'égalité d'accès aux soins. L'acteur de santé a deux options pour identifier l'offre la plus adaptée à la situation de son patient : utiliser la fonction de recherche associée au ROR ; ou utiliser des applications métier d'orientation, de coordination, de régulation qui s'appuient sur les données du ROR.

Compte tenu des enjeux, la direction générale de l'offre de soins (DGOS), a créé un programme national, le programme ROR qui accompagne les acteurs de santé pour converger vers une description harmonisée de l'offre de santé et garantit à ces acteurs l'accès à une image nationale de cette offre. De façon concrète, le programme doit définir et mettre en œuvre les conditions pour :

- qu'un acteur de santé qui se connecte sur le service de recherche de son ROR régional puisse accéder à l'offre de santé sur l'ensemble du territoire national ;
- qu'une application qui a besoin de la description de l'offre de santé régionale ou nationale puisse accéder à l'ensemble des ROR de façon normalisée (flux d'échange normalisé).

La convergence autour du ROR évite ainsi la multiplication des référentiels de description de l'offre de santé dans les applications métiers, permet de concentrer les efforts de peuplement sur un référentiel unique et favorise l'interopérabilité des SI qui s'appuient ainsi sur une vision harmonisée de l'offre de santé.

LES ENJEUX POUR LES ETABLISSEMENTS

Le ROR permet à un établissement d'exposer son offre notamment auprès de nouveaux acteurs susceptibles de lui adresser leurs patients. Demain le ROR alimentera des applications comme Via Trajectoire (orientation en SSR), le SI des SAMU ou des portails grands publics. Ainsi, pour que l'offre de l'établissement soit référencée dans ces applications qui facilitent l'orientation du patient vers la bonne prise en charge, les établissements doivent tenir à jour cette offre dans le ROR.

Les données de description opérationnelle de l'offre de santé sont saisies dans le ROR par les établissements qui sont responsables de leur complétude et de leur qualité. L'enjeu particulier pour les GHT est :

- de mettre en place des processus qui favorisent la mise à jour des données dans l'ensemble des établissements qu'ils regroupent et de s'assurer de la cohérence des offres exposées ;
- de favoriser l'utilisation du ROR par les professionnels de santé car la qualité s'acquiert par l'usage.

POUR EN SAVOIR PLUS

- Site ASIP Santé : ***esante.gouv.fr/services***

S'ouvrir sur les SI de santé externes

FR S1

LES PROFESSIONNELS DE SANTE UTILISENT DE PLUS EN PLUS DES PORTAILS ET TELESERVICES

Ces portails et téléservices – qui peuvent être **nationaux** ou **régionaux –** permettent :

- de partager ou échanger des données de santé ;
- d'effectuer des déclarations réglementaires en ligne ;
- de collecter des données administratives en ligne ;
- de se renseigner sur l'offre de soins et orienter le patient…

Les professionnels de santé accèdent généralement à ces services via un portail web. Parfois, l'accès est possible directement à partir des logiciels métier, sous la forme de téléservices intégrés. Cette intégration facilite leur utilisation au quotidien.

Quelques exemples de portails et téléservices nationaux et régionaux existants pour les établissements de santé sont présentés ci-après. Ceux faisant l'objet d'une fiche dédiée sont marqués par une *.

LES SERVICES DE PARTAGE ET D'ECHANGE DE DONNEES DE SANTE

Exemple

- Le DMP (dossier médical partagé, porté par la CNAMTS)* permet le partage des documents nécessaires à la coordination des soins. Il est accessible par le patient et ouvert à tout professionnel de santé impliqué dans la prise en charge du patient.
- Le DP (dossier pharmaceutique, porté par le CNOP) recense les médicaments délivrés au patient au cours des quatre derniers mois. Accessible aux pharmacies et à certains médecins hospitaliers, il a pour objectif de repérer les risques d'interaction médicamenteuse.
- Les systèmes de transmission et d'archivage des images médicales (PACS, portés par les MOA régionales ou des établissements) permettent aux professionnels de santé de partager ces images.
- Le système MSSanté (messageries sécurisées en santé, portées par l'ASIP Santé)* offre aux professionnels un moyen sécurisé d'échange d'informations.

LES SERVICES DE DEMATERIALISATION DES DEMARCHES REGLEMENTAIRES

Exemple

- CERT-DC (porté par la DGS et l'INSERM) permet aux professionnels de santé de déclarer les décès.
- Le portail des signalements (PSIG, porté par la DGS et l'ASIP Santé) permet aux professionnels de santé et au public de déclarer des événements sanitaires indésirables, qui seront ensuite remontés aux ARS, à l'INSERM, à l'ANSM, aux centres antipoison, aux centres régionaux de pharmacovigilance…
- E-DO (porté par l'ANSP) permet aux professionnels de santé de déclarer certaines maladies à déclaration obligatoire.

- E-FIT (porté par l'ANSM) permet aux professionnels de santé en charge de l'hémovigilance de déclarer les incidents transfusionnels.

- E-Saturne (en projet, porté par l'ANSM) permet aux professionnels de santé de réaliser une demande d'autorisation temporaire d'utilisation (ATU) nominative de médicaments.

- SI-VIC (en projet, porté par l'ASIP Santé) permet aux services d'urgences des établissements de santé de recenser les victimes d'attentat.

- Syrenad (porté par l'agence de la biomédecine) permet le recueil des donneurs / receveurs de moelle osseuse.

- Cristal (porté par l'agence de la biomédecine) permet le recueil des donneurs / receveurs d'organes.

LES SERVICES DE COLLECTE DES INFORMATIONS ADMINISTRATIVES

Exemple

- CDR/CDRI (porté par la CNAMTS) permet d'accéder aux droits du patient vis-à-vis de son organisme d'assurance maladie obligatoire.

- Les téléservices associés au projet rembour-sement des organismes complémentaires (ROC, portés par les organismes d'assurance maladie complémentaire) permettent d'accéder aux droits du patient vis-à-vis de son organisme d'assurance maladie complémentaire et de simuler puis calculer la part prise en charge par ce dernier.

- L'espace pro ameli.fr (porté par la CNAMTS) permet aux professionnels de santé d'accéder aux services de l'Assurance-Maladie.

LES AUTRES SERVICES

Exemple

- Le ROR (répertoire opérationnel des ressources, porté par les ARS avec les MOA régionales)* décrit en détail l'offre de soins pour permettre aux professionnels de santé d'identifier la structure ou le professionnel de santé le plus adapté à la situation du patient.

- Les services de télémédecine.

- Les portails régionaux (portés par les MOA régionales) apportent aux usagers et aux professionnels de santé un certain nombre de services (plateforme de prise en charge de parcours de soins complexes, gestion / préparation de l'hospitalisation,…).

S'intégrer dans le cadre commun des projets e-santé de sa région

FR S2

UN CADRE POUR GARANTIR A TOUS LES PROFESSIONNELS UN SOCLE COMMUN MINIMUM DE SERVICES NUMERIQUES EN SANTE SUR LEUR TERRITOIRE.

La stratégie nationale de santé présentée par la Ministre de la santé et des affaires sociales en septembre 2013 vise à organiser les soins du patient dans le cadre d'une médecine de parcours reposant sur une coopération de l'ensemble des professionnels.

Elle identifie le numérique comme un facteur clé de soutien à la mise en place de ces parcours, et plus largement, à l'amélioration de la qualité et de la sécurité des soins et à la modernisation des pratiques.

Le cadre commun des projets e-santé - aussi appelé cadre d'urbanisation des projets de e-santé - a été construit avec tous les acteurs concernés.

Il a pour objectif de garantir la cohérence et l'efficience des actions régionales de promotion et d'usage de services numériques. Il précise :

- les référentiels qui s'appliquent à tous les projets de e-santé ;
- le socle commun minimum de services à proposer dans les territoires ;
- les principes de conduite de projets devant s'appliquer aux projets de e-santé.

Publié en mai 2016[9], il s'impose dans les territoires sous le pilotage des agences régionales de santé (ARS).

UN SOCLE COMMUN MINIMUM DE SERVICES DEPLOYE ET UTILISE DANS L'ENSEMBLE DES REGIONS FRANÇAISES

La première version du socle commun impose la mise en œuvre dans tous les territoires des services numériques suivants :

- **Pour le partage de données de santé** :
  - le dossier médical partagé (DMP) ;
  - un dossier communiquant en cancérologie (DCC) ;
  - les solutions de partage d'images médicales (PACS).
- **Pour l'échange sécurisé de données de santé** :
  - le service de messageries sécurisées de santé (MSSanté).
- **Pour la présentation de l'offre de soins d'un territoire et l'orientation des patients** :
  - un répertoire opérationnel des ressources (ROR) ;
  - un service d'orientation et d'aide au placement des patients et usagers.
- **Pour la prise en charge à distance et coordonnée du patient :**
  - des services de télémédecine.

D'autres services viendront enrichir ce socle commun dans ses versions suivantes. D'ores et déjà certaines régions proposent des services complémentaires au socle commun.
Les établissements, et en particulier les GHT, en tant que point de passage clé dans le parcours des patients, doivent prévoir, dans leur schéma directeur, d'utiliser ces services et de respecter les référentiels du cadre commun s'ils exposent eux-mêmes des services.

POUR EN SAVOIR PLUS

- Site de l'ASIP Santé : ***esante.gouv.fr***

[9] Cf. circulaire : ***http://rohlim.fr/sites/default/files/files/DCC/Esante%20-%20AG%202016-06-28%20pj3%20instruction%20cadre%20commun.pdf***

Partager les informations de santé utiles à la coordination des soins via le DMP

FR
S3

UN SERVICE NATIONAL DE PARTAGE DE DOCUMENTS DE SANTE POUR FACILITER LA CONTINUITE DES SOINS

La prise en charge continue et coordonnée du patient par l'ensemble des acteurs nécessite que l'information, utile à la coordination des soins, soit partagée par l'ensemble des professionnels de santé qu'ils exercent au sein d'un établissement de santé, d'un GHT, d'une structure médico-sociale ou en libéral.

Le DMP (dossier médical partagé) **permet en effet de partager, en toute sécurité, les documents produits par les différents professionnels acteurs de la prise en charge :** synthèse médicale, lettre de liaison, compte rendu d'hospitalisation, compte-rendu de radiologie, résultats d'analyses de biologie, documents relatifs aux antécédents et allergies… Il constitue ainsi le carnet de santé électronique du patient.

Inscrit dans la loi[10], le DMP est un service national sécurisé, accessible aux professionnels de santé autorisés (par le biais de leurs logiciels métiers « DMP compatibles » ou à défaut, via le portail internet dmp.gouv.fr) **et au patient** (par le portail internet).

Lancé en 2010 par l'ASIP Santé et déployé dans certains territoires avec l'appui des ARS, des GCS e-santé et autres partenaires en région, le DMP est administré depuis le 4 juillet 2016[11] par la caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) qui en assure le déploiement sur l'ensemble du territoire français.

UTILISER LE DMP

Au 1er juillet 2016, plus de 730 établissements et structures de santé utilisent le DMP, dans le cadre d'initiatives individuelles, de démarches d'accompagnement territoriales ou dans la continuité du programme Hôpital Numérique[12].

Le schéma directeur des SI des établissements, et en particulier celui des GHT, doit veiller à ce que le futur logiciel portant le dossier patient soit « DMP compatible »[13] (directement ou via une passerelle DMP compatible) et permette d'intégrer au mieux, dans la pratique quotidienne des professionnels de santé, les modalités d'alimentation et de consultation du DMP.

Dans l'attente de la mise en œuvre du SI convergent, les GHT peuvent utiliser le DMP comme outil de coordination des soins entre les professionnels de santé intervenant dans les différents établissements constitutifs du GHT. Dans l'attente d'avoir un dossier patient commun au sein des GHT, le DMP peut permettre d'assurer un premier niveau de partage, et ainsi faciliter la continuité et la coordination des soins des patients suivis dans plusieurs établissements du GHT.

Pour en savoir plus

- Site du DMP : ***www.dmp.gouv.fr***
- Guide pratique du projet DMP en établissement (2012) : ***www.dmp.gouv.fr/documentation/guide-dmp-en-es***

[10] Loi n° 2004-810 du 13 août 2004
[11] Décret n° 2016-914 du 4 juillet 2016

[12] cf. domaine prioritaire 2 « DPII (dossier patient informatisé et interopérable) et communication extérieure » impliquant la « DMP compatibilité » du DPI et la publication des comptes rendus d'hospitalisation dans le DMP.
[13] Cf. guide méthodologique « Stratégie, optimisation et gestion commune d'un système d'information convergent d'un GHT ».

Echanger les données de santé avec ses correspondants, via MSSanté

FR
S4

UNE MESSAGERIE SECURISEE POUR FACILITER LA COORDINATION ET LA CONTINUITE DES SOINS

La prise en charge continue et coordonnée du patient par l'ensemble des acteurs nécessite que tous les professionnels - qu'ils exercent au sein d'un établissement de santé, d'un GHT, d'une structure médico-sociale ou en libéral - puissent échanger entre eux les données de santé des patients qu'ils prennent en charge (notamment via la lettre de liaison). Pour gagner du temps, ces échanges se font de plus en plus par email.

Ces échanges doivent se faire en utilisant une messagerie sécurisée de santé.

L'espace de confiance MSSanté est défini. Toutes les messageries intégrant cet espace de confiance en répondant aux exigences techniques requises permettent aux professionnels de santé d'échanger des données de santé de façon sécurisée en garantissant la confidentialité, la traçabilité et l'intégrité de ces échanges.

Des travaux sont également en cours pour que les professionnels du secteur médico-social habilités à échanger des données de santé[14] puissent également bénéficier de ces messageries.

Le système MSSanté permet aux opérateurs publics ou privés (établissements de santé, industriels, opérateurs de solutions régionales, autres opérateurs) **d'intégrer l'espace de confiance MSSanté.** Il se caractérise par :

- Un annuaire MSSanté[15] ayant vocation à référencer l'ensemble des professionnels habilités à échanger des données de santé.
- Une liste blanche de domaines qui regroupe l'ensemble des domaines de messageries des opérateurs autorisés à échanger dans l'espace de confiance MSSanté.
- Des référentiels permettant aux industriels de développer des offres interopérables.

L'espace de confiance MSSanté a vocation à intégrer l'ensemble des solutions de messagerie sécurisée existantes et de les rendre interopérables. Il appartient à ces solutions de se connecter à l'espace de confiance pour être en mesure de tirer avantage de l'interopérabilité.

[14] cf. article L.11110-4 du code de la santé publique et le décret n° 2016-994 du 20 juillet 2016

[15] Composante de l'annuaire santé – cf. fiche R2.

INTEGRER LA MSSANTE DANS LE SCHEMA DIRECTEUR SI

L'instruction DGOS du 23 décembre 2014 relative à l'usage de la messagerie sécurisée MSSanté dans les établissements de santé demande à tous les établissements de santé d'intégrer l'espace de confiance MSSanté.

Les établissements, et en particulier les GHT, doivent donc, dans leur réflexion sur le schéma directeur des SI, intégrer ce dispositif.
Pour faciliter l'usage de cette messagerie au quotidien par les professionnels de santé, il est fortement conseillé qu'elle soit intégrée dans le SIH : l'envoi des documents issus du DPI vers les correspondants peut ainsi être automatisé (via des boites aux lettres applicatives), évitant l'envoi des documents papier par courrier.
Pour cela, les documents produits par les DPI doivent être accompagnés de métadonnées (identifiant patient, type de document, producteur…) afin de faciliter le traitement des documents par les destinataires.

L'intégration de MSSanté dans le cas spécifique des GHT peut s'envisager de deux façons :

- Soit chaque établissement du GHT met en place sa propre solution. Les messageries du dispositif MSSanté étant interopérables, les établissements du GHT ayant déjà une solution compatible peuvent la conserver.

- Soit l'installation de la messagerie se fait au niveau du groupement. Dans ce cas, il est nécessaire de mener une réflexion, par exemple sur les sujets suivants (liste non exhaustive) :

  - Sur le nom de domaine (celui du GHT ? celui de chaque établissement ?). Pour les établissements déjà dotés d'un dispositif MSSanté, cela dépendra des possibilités offertes par le contrat souscrit auprès de leur opérateur actuel.

  - Sur la solution technique (l'établissement support devient-il opérateur MSSanté pour l'ensemble du groupement? Le GHT passe-t-il par un opérateur tiers MSSanté ?…).

DEPLOYER MSSANTE

L'ASIP Santé accompagne, sur 2017, les établissements de santé et les GHT qui le souhaitent dans le déploiement de MSSanté.
Elle peut ainsi les aider à :

- organiser une réunion de lancement dans le GHT / l'établissement de santé ;

- réaliser le diagnostic interne ;

- étudier les modalités de raccordement technique ;

- assurer le déploiement fonctionnel et favoriser les usages au quotidien de la messagerie ;

- amorcer la communication autour de MSSanté (en interne et vis-à-vis des partenaires extérieurs).

POUR EN SAVOIR PLUS

- Site MSSanté : ***https://www.mssante.fr/comprendre-mssante***
- Mail de l'équipe de déploiement MSSanté : ***mssante.es@sante.gouv.fr***

Utiliser la certification Qualité Hôpital Numérique

FR S5

L'élaboration des schémas directeurs SI impliquent une **analyse de la maturité** des systèmes de management de la qualité (SMQ) des industriels fournisseurs de logiciels.

Cette analyse peut être réalisée, lors de la réalisation du diagnostic de l'existant, pour évaluer le SMQ des fournisseurs des établissements. Elle peut également être réalisée lors de la réflexion autour de la cible, pour évaluer les processus de management de la qualité des fournisseurs envisagés.

LA CERTIFICATION QUALITE HOPITAL NUMERIQUE, UN MOYEN D'EVALUER LE SMQ DES INDUSTRIELS

La certification qualité hôpital numérique (QHN) garantit aux établissements de santé que :

- les logiciels sont testés avant leur installation en production ;
- les déploiements sont efficaces et réalisés par des équipes formées et stables ;
- le support est réactif ;
- l'industriel donne de la visibilité sur l'évolution de ses produits.

Pour cela, elle inclut des critères relatifs à :

- la conception, au développement et à l'évolution du produit (tests en usine, maintenance corrective…) ;
- la gestion des services de production (fonctionnement en mode dégradé, garanties…) ;
- la gestion de projets (accompagnement…) ;
- l'interopérabilité ;

Le certificat qualité hôpital numérique est délivré par des organismes certificateurs accrédités par le COFRAC signataires d'une convention avec l'ASIP Santé.
L'ASIP Santé publie la liste des industriels certifiés qualité hôpital numérique

LA CERTIFICATION QUALITE HOPITAL NUMERIQUE S'ADRESSE A L'ENSEMBLE DES INDUSTRIELS

- éditeurs de logiciels (produits standard sur étagère, progiciels) ;
- développeurs de logiciels (logiciels à façon) ;
- intégrateurs de logiciels (distributeur d'applications métiers et/ou producteurs de systèmes d'intégration destinés à être commercialisés) ;
- fournisseurs de solution en mode service (SaaS).

Le référentiel qualité hôpital numérique[16] s'inscrit dans le cadre d'une certification de système de management de la qualité (SMQ) suivant les normes ISO 9001 ou ISO 13485. Ces normes sont spécifiées par des exigences complémentaires pour tenir compte des particularités des solutions à destination des établissements de santé.

[16] Référentiel Qualité Hôpital Numérique
Version 1.1 – octobre 2015
http://esante.gouv.fr/services/qualite-hopital-numerique/espace-etablissements-de-sante

Les établissements peuvent ainsi inciter leurs industriels partenaires à s'engager dans la démarche de certification qualité hôpital numérique.
Les établissements peuvent aussi évaluer le SMQ de leurs fournisseurs de système d'information de santé à partir des exigences du référentiel QHN.

Si un établissement souhaite s'assurer de la qualité de services garantie par la certification QHN, il peut ajouter cette exigence dans les critères contenus dans son cahier des charges lors d'un appel d'offres.

COMMENT UN INDUSTRIEL PEUT-IL ETRE CERTIFIE QUALITE HOPITAL NUMERIQUE ?

Les industriels souhaitant devenir certifiés Qualité Hôpital Numérique, peuvent contacter l'un des organismes conventionnés avec l'ASIP Santé.
La liste ci-dessous correspond à ces organismes conventionnés à date.

- AFNOR - ***http://www.boutique-certification.afnor.org/certification/qualite-hopital-numerique***
- Apave Certification - ***http://www.apave-certification.com/***
- Bureau VERITAS - ***www.bureauveritas.fr/certification***
- SGS - ***http://www.sgsgroup.fr***

POUR EN SAVOIR PLUS

- Site certification qualité hôpital numérique : ***esante.gouv.fr/services***

Simplifier la chaîne accueil – facturation – recouvrement en automatisant et dématérialisant les démarches administratives

FR S6

LE PARCOURS PATIENT ADMINISTRATIF: UNE SIMPLIFICATION NECESSAIRE

Lecture des droits de l'assuré, envoi de factures sous format papier, édition de relances pour le recouvrement….Autant de tâches administratives, à faible valeur ajoutée, que les équipes administratives des établissements de santé prennent en charge.

CES TACHES PEUVENT ETRE AUTOMATISEES ET DEMATERIALISEES

Le programme Simphonie (simplification du parcours patient hospitalier et numérisation des informations échangées), piloté par la DGOS, vise à **simplifier le circuit administratif** du patient, **par le biais de l'automatisation des tâches et la dématérialisation des échanges**.

Ce programme comprend plusieurs chantiers, couvrant l'ensemble du parcours patient, à titre d'exemples :

- **la récupération automatique des droits auprès de l'assurance-maladie obligatoire** (AMO), via l'intégration du téléservice CDRI porté par la CNAMTS dans les logiciels de gestion administrative du patient (GAP) ;
- **la récupération automatique des droits auprès de l'assurance-maladie complémentaire** (AMC), via l'intégration des téléservices ROC portés par les organismes AMC dans les logiciels GAP ;
- **l'envoi dématérialisé des factures AMC et des retours associés** via l'extension des normes de télétransmission B2 et NOEMIE au circuit de facturation AMC.
- **du recouvrement automatisé du reste à charge patient**, via le dispositif Diapason, permettant l'enregistrement, en lien avec la GAP, des coordonnées bancaires du patient par un tiers de confiance afin que son compte soit débité, une fois le montant de la facture connu.
- **de la promotion des initiatives de modernisation des démarches administratives** (prise de rendez-vous en ligne, préadmission en ligne, enregistrement sur bornes…).
- **du pilotage intégré dans la GAP de l'ensemble de la chaine des recettes**, via des indicateurs, des états et des listes de travail automatisés.

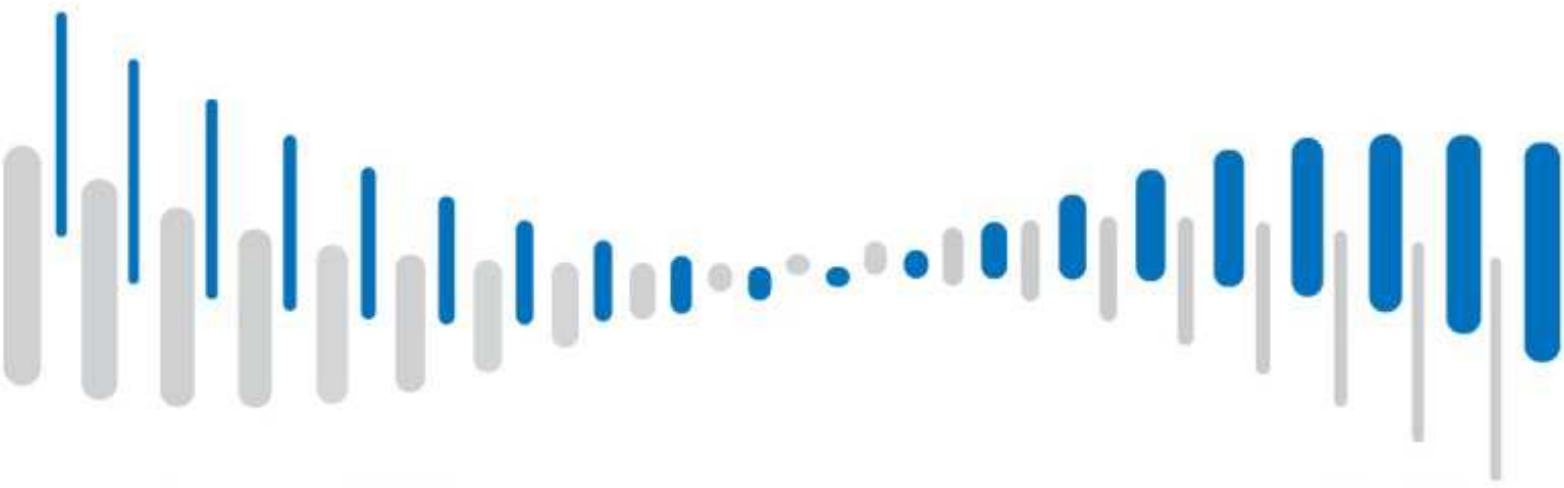
Ces chantiers sont en cours d'expérimentation ou de déploiement. Ils permettront aux établissements de santé de **repenser leur parcours patient administratif et l'organisation de leur chaîne d'accueil – facturation – recouvrement.**

Ces évolutions se traduiront par des gains, en termes de qualité de la prise en charge administrative du patient, **d'efficacité de gestion** et de **sécurisation des recettes.**

La prise en compte de ces évolutions dans le schéma directeur SI des établissements et en particulier des GHT est donc fondamentale afin de rendre possible cette transformation de la chaîne accueil – facturation – recouvrement.

POUR EN SAVOIR PLUS

- Page Simphonie – Ministère des Affaires Sociales et de la Santé : ***http://social-sante.gouv.fr/professionnels/gerer-un-etablissement-de-sante-medico-social/performance-des-etablissements-de-sante/simphonie/article/simphonie***



L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

esante.gouv.fr
ASIP Santé
9, rue Georges Pitard – 75015 Paris
T. +33 (0)1 58 45 32 50
Du lundi au vendredi de 8h30 à 18h30 (hors jours fériés)