

# Cadre d'urbanisation sectoriel

Modèle d'identification des professionnels du secteur santé

26 avril 2017 - Version 1.2



## Table des matières

1	Contexte .....	4
2	Pourquoi un modèle national d'identification .....	4
3	Principes généraux .....	4
3.1	Définitions .....	4
3.2	Identification des acteurs dans les échanges .....	6
4	Recommandations pour la gestion des identifiants et d'un annuaire .....	7
4.1	Préambule .....	7
4.2	Recommandations.....	8
5	Cas des GHT – recommandations pour la mise en œuvre d'un annuaire centralisé .....	10
6	Gestion des cartes CPS – Focus sur les GHT .....	11

# 1 Contexte

En complément des travaux menés sur le référentiel d'identification des acteurs dans le cadre de la PGSSI-S, l'ASIP Santé propose au travers du présent document de poser des recommandations relatives aux principes d'identification des professionnels au sein des structures de santé, au-delà des seuls acteurs concernés par l'accès aux données de santé.

Le présent document s'inscrit dans le corpus documentaire du cadre d'urbanisation sectoriel publié par l'ASIP Santé.

Il a pour objet de décrire un modèle partagé d'identification des professionnels du secteur santé.

N.B : la présente version 1.2 fait suite à un alignement de terminologie des identifiants avec la PGSSI-S

## 2 Pourquoi un modèle national d'identification

Chaque structure de santé est amenée à gérer l'identification des intervenants au sein de son périmètre de responsabilité, qu'il s'agisse de permettre de contrôler l'accès au système d'information, aux locaux et plus généralement à l'ensemble des services « domotiques » (parkings, restaurant d'entreprise...).

L'objectif du modèle national d'identification est de partager un socle commun de bonnes pratiques permettant, à partir de concepts homogènes de gestion d'identité pour l'ensemble des professionnels intervenant au sein d'une structure, de répondre aux besoins d'attributions de droits et aux besoins potentiels de partage ou échanges d'information entre périmètres de responsabilité.

## 3 Principes généraux

### 3.1 Définitions

Les concepts utilisés dans le présent document sont définis dans le « Référentiel d'identification des acteurs sanitaires et médico-sociaux » de la PGSSI-S<sup>1</sup> (Politique Générale de la Sécurité des Systèmes d'Information de Santé).

On rappelle toutefois ici les concepts d' « Autorité d'Enregistrement », d' « Autorité d'Affectation », d' « identifiant public » et d' « identifiant privé » en les complétant et les illustrant.

<sup>1</sup> Cf. <http://esante.gouv.fr/> rubrique « Politique Générale de la Sécurité des Systèmes d'Information de Santé »

- **Autorité d’Affectation** : Dans le cadre de la PGSSI-S, la personne portant la responsabilité d’un référentiel d’identité est désignée sous le terme d’Autorité d’Affectation.

L’Autorité d’Affectation est en charge de la définition de la finalité du référentiel d’identité, du périmètre des personnes pouvant ou devant être enregistrées dans le référentiel d’identité, des règles d’attribution d’un identifiant à une personne, du format de l’identifiant géré, à l’exception de ceux de ces aspects qui seraient déjà fixés par voie légale ou réglementaire.

Une Autorité d’Affectation porte la responsabilité d’un seul référentiel d’identité, et réciproquement un référentiel d’identité est sous la responsabilité d’une seule Autorité d’Affectation.

Exemple : cas d’un médecin :

- l’Autorité d’Enregistrement est l’Ordre des médecins ;
- l’Autorité d’Affectation de l’identifiant public RPPS est l’ASIP Santé.

- **Autorité d’Enregistrement** : Dans le cadre de la PGSSI-S, une Autorité d’Enregistrement est une structure organisationnelle qui assume, pour le compte d’une Autorité d’Affectation, la responsabilité de la collecte, de la validation des traits d’identité des personnes préalablement à l’attribution d’un identifiant et à l’enregistrement de ces données d’identité dans un référentiel d’identité.

L’Autorité d’Enregistrement est également responsable de la mise à jour des traits d’identité sur la durée de vie de l’identifiant.

La liste des traits d’identité enregistrés par l’Autorité d’Enregistrement et le mode de vérification de l’identité des personnes lors de l’enregistrement sont propres à chaque référentiel d’identité et sont fixées par ou avec l’Autorité d’Affectation.

La fonction d’Autorité d’Enregistrement peut être assurée par l’Autorité d’Affectation elle-même, ou être délégué à une ou plusieurs personnes, selon l’organisation prévue pour la mise en œuvre du référentiel d’identité.

Le périmètre d’action des Autorités d’Enregistrement peut relever du niveau national (ex. les ARS pour le répertoire FINESS, référentiel d’identité national) ou du niveau local (ex. un hôpital enregistrant ses salariés au sein d’un annuaire local).

- **Identifiant public** : l’identifiant public, **de portée nationale**, est un identifiant attribué à la suite de l’enregistrement dans un référentiel d’identité national par une Autorité d’Enregistrement et sous la responsabilité d’une Autorité d’Affectation dûment habilitées par une autorité de l’Etat. Pour les professionnels de santé, il s’agit du n° RPPS ou du n° ADELI selon les professions<sup>2</sup>.

---

<sup>2</sup> Au 1<sup>er</sup> janvier 2017 : N° RPPS pour les médecins, chirurgiens-dentistes, sages-femmes, pharmaciens et masseur-kinésithérapeutes, n° ADELI pour les autres professions auxiliaires de santé.

- **Identifiant privé** : l'identifiant privé, **de portée locale**, est un identifiant attribué à la suite de l'enregistrement par une Autorité d'Enregistrement pour un référentiel autre qu'un référentiel d'identité national.

A titre d'exemple, l'Autorité d'Enregistrement peut être, sans que cette liste soit exhaustive :

- un établissement de santé qui met en place un annuaire interne ayant vocation d'attribuer un identifiant aux salariés ainsi qu'aux intervenants externes ;
- un GHT qui souhaite mettre en œuvre un processus et une gestion d'identité communs à l'ensemble du GHT ;
- un fournisseur d'appareillage médical (optique ou audioprothèse) qui souhaite mettre en œuvre un annuaire commun à toutes ses enseignes ;
- un laboratoire d'analyses médicales...

Les traits d'identité et toute autre information associés aux acteurs sont collectés et rassemblés sous la responsabilité de l'Autorité d'Enregistrement. Elles n'ont de sens que dans le périmètre de responsabilité de l'Autorité d'Enregistrement. L'Autorité d'Affectation attribue l'identifiant privé, de portée locale, à l'acteur.

L'Autorité d'Affectation peut être confondue avec l'Autorité d'Enregistrement ou bien s'appuyer sur plusieurs Autorités d'Enregistrement. A titre d'exemple dans le cadre d'un GHT, sans que ce soit une règle, chaque établissement membre du GHT peut être Autorité d'Enregistrement de ses salariés et le rôle d'Autorité d'Affectation de l'identifiant être dévolu à l'un des membres du GHT, l'établissement support par exemple ; l'identifiant privé est alors défini sur l'ensemble du périmètre du GHT.

Une même personne physique ne disposant pas d'un identifiant public, intervenant dans le périmètre de deux Autorités d'Affectation différentes sera dotée de deux identifiants distincts et dépendra d'Autorités d'Enregistrement distinctes.

N.B. : l'identifiant public ou l'identifiant privé ne sont pas nécessairement utilisés en tant que nom d'utilisateur (« login ») pour se connecter au système d'information. A titre d'exemple, le nom d'utilisateur d'un professionnel de santé disposant d'un identifiant public RPPS peut être une chaîne de caractères mnémotechnique.

## 3.2 Identification des acteurs dans les échanges

### Partage ou échanges de données de santé à caractère personnel

Dès lors qu'il y a partage ou échange de données de santé à caractère personnel en dehors du périmètre de couverture de l'Autorité d'Affectation, les acteurs impliqués dans le processus doivent être clairement identifiés.

Concernant les professionnels disposant d'un identifiant public, le CI-SIS<sup>3</sup> et la PGSSI-S imposent d'identifier le professionnel par son identifiant public (n° RPPS ou n° ADELI).

Concernant les professionnels ne disposant pas d'un identifiant public (par exemple, un praticien à diplôme étranger « faisant fonction d'interne »), l'identifiant privé doit être étendu à une portée nationale sous la forme :

« Identifiant de la structure Autorité d'Affectation » / « identifiant privé »

#### **Echanges hors partage ou échanges de données de santé**

Concernant l'identification des acteurs, il est recommandé d'adopter les mêmes règles que dans le cas d'un échange de données de santé à caractère personnel.

## **4 Recommandations pour la gestion des identifiants et d'un annuaire**

### **4.1 Préambule**

Au sein d'un système d'information, un acteur peut avoir besoin d'utiliser différents identifiants en fonction des contraintes locales, certaines applications pouvant par exemple imposer une forme d'identifiant spécifique incompatible avec les autres composants du système d'information.

Il importe donc qu'au sein d'un périmètre de gestion coordonnée des identifiants des acteurs (Etablissement de santé, GHT...) soit attribué à tout acteur un « identifiant principal » sur lequel puisse être fédéré l'ensemble des identifiants associés à cet acteur, notamment son identifiant public (n° RPPS ou n° ADELI) ainsi que les noms d'utilisateurs de connexion au SI (« login »).

Au sein de ce périmètre, le choix de la forme et des processus d'attribution de l'identifiant principal est libre. Par exemple, un établissement peut utiliser le matricule RH en tant qu'identifiant principal de ses salariés et un numéro de séquence pour les intervenants externes dont l'enregistrement dans l'annuaire est nécessaire.

La mise en œuvre d'un **référentiel d'identité centralisé** prend tout son sens pour fédérer tous les identifiants d'un acteur autour d'un identifiant principal afin :

- de réduire les risques de doublons<sup>4</sup> et de collision<sup>5</sup> ;

<sup>3</sup> CI-SIS : Cadre d'Interopérabilité des Systèmes d'information de santé.

<sup>4</sup> Doublet : Il y a doublet d'identifiants lorsque plusieurs identifiants sont attribués à une même personne dans par une Autorité d'Affectation.

<sup>5</sup> Collision : Il y a collision d'identifiants lorsqu'un même identifiant a été attribué à deux personnes différentes par une Autorité d'Affectation.

- de maîtriser les processus d'entrée et sortie et de gestion des habilitations.

En termes de bonnes pratiques, pour les salariés, l'annuaire d'identité doit être adossé à l'annuaire des ressources humaines.

## 4.2 Recommandations

### Maintenir dans le temps les liens entre les identifiants

L'association entre l'identifiant principal et les autres identifiants doit être conservée dans le temps, ainsi que l'historique des modifications, afin de permettre dans la durée l'imputabilité des actions effectuées par l'acteur concerné

### Maintenir dans le temps le lien avec l'identifiant public

Si l'acteur concerné dispose d'un identifiant public (n° RPPS ou n° ADELI selon la profession concernée<sup>6</sup>) ce dernier doit obligatoirement être enregistré dans le référentiel d'identité centralisé, et le cas échéant, en fonction des contraintes techniques locales, dans les référentiels d'identité propre à chaque SI. Il sera notamment nécessaire pour tout échange en dehors du périmètre de l'Autorité d'Affectation locale, la production d'un document de santé, pour répondre aux obligations réglementaires ou administratives...

A cet effet, le recours aux services de publication des données des professionnels de santé (Annuaire Santé<sup>7</sup>) mis en œuvre par l'ASIP Santé est opportun pour vérifier les identifiants communiqués par les professionnels et mettre à jour dans l'annuaire toute information utile mise à disposition par ces services de publication, voire vérifier les qualifications de ces professionnels, notamment lors du processus d'embauche.

### Homogénéiser les règles de gestion d'identité pour tous les acteurs

Il est recommandé de centraliser au sein du référentiel d'identité les acteurs internes (salariés) et les intervenants externes afin d'homogénéiser les règles de collecte et de validation des traits d'identité, de gestion d'habilitation et de contrôle d'accès (IAM<sup>8</sup>) pour tous les acteurs : de l'accès au système d'information au contrôle d'accès physique (badges, journal d'entrées-sorties) en passant par les services domotiques (parking, restaurant d'entreprise...).

Les règles de gestions d'identité doivent intégrer les processus et contrôles prévenant (et corrigeant) l'apparition de doublons et de collisions d'identifiant principal<sup>9</sup>.

### Baser la gestion des habilitations sur des rôles métier

<sup>6</sup> Un professionnel de santé ne peut disposer à la fois à un instant « t » d'un numéro RPPS opérationnel et d'un numéro ADELI opérationnel. Progressivement, toutes les professions migrent vers l'attribution d'un numéro RPPS en remplacement du numéro ADELI.

<sup>7</sup> <http://esante.gouv.fr/services>

<sup>8</sup> IAM : « Identity and Access Management »

<sup>9</sup> A titre d'exemple, deux systèmes RH historiquement indépendants au sein d'un GHT peuvent avoir attribué un même numéro de matricule à des professionnels différents. Leur distinction ne peut se faire qu'en leur attribuant des identifiants principaux différents.



Il est recommandé d'associer à tout acteur un ou plusieurs « métier » exercé(s) au sein de l'organisation sur lesquels peuvent s'appuyer les processus d'habilitation et de contrôle d'accès, l'attribution de ce métier est assurée sous la responsabilité de l'Autorité d'Enregistrement locale.

A cet effet, le « répertoire des métiers de la Fonction Publique Hospitalière »<sup>10</sup> établi par la DGOS peut constituer une nomenclature de référence, complétée si nécessaire par des métiers spécifiques à l'organisation, notamment au niveau d'un GHT.

N.B. : la profession de l'acteur indiquée dans les référentiels nationaux (RPPS ou ADELI) est une information distincte du métier exercé au sein de l'organisation. Elle doit être enregistrée à ce titre dans l'annuaire. A titre d'exemple, la profession garantie par le référentiel national (RPPS) est « médecin », le métier exercé au sein de l'établissement est « Encadrant (e) de département d'information médicale ».

L'attribution d'un métier à un acteur permet notamment :

- de se mettre en capacité d'attribuer des droits « primaires » aux acteurs : accès aux applications (et le cas échéant les droits fins dans ces applications si la gestion centralisée est possible), accès physiques au site, aux locaux, etc.;
- d'identifier les acteurs dont le métier implique potentiellement un accès à des données de santé à caractère personnel pour lesquels des exigences de sécurité particulières doivent être respectées : respect de la PGSSI-S, éventuellement dotation de moyens d'authentification spécifiques...

### **Assurer la cohérence avec l'identification portée par les cartes de la famille CPS**

De nombreux établissements de santé demandent pour au moins une partie de leur personnel des cartes CPE<sup>11</sup> délivrées par l'ASIP Santé. Les cartes CPE permettent notamment l'accès aux télé-services de consultation des droits des bénéficiaires de l'assurance maladie.

D'autres établissements, ou regroupements d'établissement, ont fait, ou feront le choix de généraliser l'usage des cartes de la famille CPS (CPS : Carte de Professionnel de Santé, CPE : Carte de Personnel d'Etablissement) en tant que moyen d'authentification au sein de leur organisation.

#### *Cartes CPS*

Les cartes CPS portent l'identifiant public des professionnel de santé, d'où l'intérêt d'avoir enregistré cet identifiant public dans l'annuaire d'établissement.

#### *Cartes CPE et CDE*

Les cartes CPE ou CDE<sup>12</sup> quant à elles portent un identifiant conforme au modèle d'extension à une portée nationale de l'identifiant privé communiqué par l'établissement lors de la demande de carte, par exemple, une carte CPE demandée au titre de la structure de numéro FINES 030780100 pour un personnel auquel a été attribué l'identifiant privé 123456, aura comme identifiant de portée nationale dans la carte CPE : 3030780100/123456.

<sup>10</sup> <http://www.metiers-fonctionpubliquehospitaliere.sante.gouv.fr/>

<sup>11</sup> CPE : Carte de Professionnel d'Etablissement

<sup>12</sup> CDE : Carte de Directeur d'Etablissement

Il importe de veiller que les identifiants locaux communiqués à l'ASIP Santé lors des demandes de carte CPE ou CDE soient choisis en cohérence avec les règles d'identification mises en œuvre par l'Autorité d'Affectation afin d'éviter des collisions d'identifiant. Une règle peut être par exemple d'utiliser l'« identifiant principal » présenté plus haut lors de la demande de carte. A défaut l'identifiant privé porté par la carte doit pouvoir être rapproché de l'identifiant principal de l'acteur.

N.B. : la longueur de l'identifiant privé communiqué lors de la demande de carte doit être limitée à 15 caractères alphanumériques.

## 5 Cas des GHT – recommandations pour la mise en œuvre d'un annuaire centralisé

L'objectif posé par le guide méthodologique publié par la DGOS<sup>13</sup> est de converger graduellement vers un système d'information mutualisé, entre autre sur la brique fonctionnelle « gestion des annuaires ».

La convergence est graduelle, les étapes principales de la démarche proposée par la présente note, en sont :

- la définition et la mise en œuvre d'un annuaire centralisé au niveau du GHT avec l'élaboration d'une politique d'identification (référentiel d'identité et processus de gestion associés) étendue sur le périmètre du GHT, dont la définition d'un « identifiant principal » au niveau du GHT.
- Le rapprochement des identifiants locaux des membres du GHT sur l'identifiant principal du GHT.

L'origine et la structure responsable de la gestion des identifiants locaux peuvent être caractérisés par un principe d'association avec l'identifiant public de l'établissement concerné (n° FINESS) afin d'éviter les collisions.

C'est une opportunité de fiabiliser les informations relatives aux professionnels de santé par rapport aux référentiels nationaux.

Cette étape est aussi l'occasion d'actualiser les annuaires et par voie de conséquence d'actualiser les habilitations et de désactiver les comptes qui ne sont plus justifiés.

- la migration progressive
  - de l'adossement des applications vers l'annuaire centralisé en termes d'enrôlement, de gestion d'habilitation et de contrôle d'accès,
  - le cas échéant, des identifiants propres à chaque établissement vers les identifiants de niveau GHT en fonction de la migration du système d'information.

---

<sup>13</sup> GHT Mode d'emploi – Guide méthodologique – Stratégie, optimisation e gestion commune d'un système d'information convergent d'un GHT Version juillet 2016

N.B. La fédération autour de l'identifiant principal de niveau GHT permet notamment de fédérer les identifiants d'une même personne intervenant dans plusieurs établissements.

### **Extension d'un identifiant privé à une identification de portée nationale**

En cible, chaque acteur intervenant au sein d'un GHT, doit être associé à un identifiant principal de niveau GHT, dans ce cadre il est proposé que l'extension d'identification à un niveau national soit portée par le FINESS de l'entité juridique de l'établissement support, qui jouerait le rôle d'Autorité d'Affectation :

<identifiant FINESS EJ de l'étab. Support>/<Identifiant de niveau GHT>

N.B. : ce principe pourra être remis en cause dans l'éventualité où le GHT soit doté d'une personnalité morale, auquel cas, c'est l'identifiant public de cette dernière qui devra être utilisé.

En phase intermédiaire, il est possible d'utiliser un référencement par rapport à l'établissement de rattachement :

<Identifiant FINESS de l'établissement>/<identifiant privé, local à l'établissement>

## **6 Gestion des cartes CPS – Focus sur les GHT**

Ce chapitre aborde la problématique d'attribution des cartes CPE aux personnes non PS exerçant dans les établissements constitutifs du GHT.

Le service de commande et de mise en opposition de cartes de l'ASIP Santé permettra de centraliser la gestion des cartes sur un regroupement d'établissements, en permettant à l'un des établissements d'effectuer les opérations pour le compte des autres.

Plusieurs politiques, non exclusives, peuvent être mises en œuvre au niveau du GHT.

### **Maintenir une attribution de cartes établissement par établissement (cas actuel).**

L'identifiant porté en carte est l'identifiant de l'établissement dans le quel exerce la personne. Dans le cas où cette personne exerce dans plusieurs établissements, il n'est pas nécessaire de lui délivrer une carte CPE par établissement. L'annuaire centralisé du GHT permet de gérer l'association entre l'identifiant porté dans la carte (<FINESS Etablissement>/<identifiant privé, local à l'établissement>) et l'identifiant principal, et de fédérer ainsi ses habilitations sur le périmètre du GHT.

Si au moment de la mise en œuvre du GHT, une personne exerçant dans plusieurs structures dispose de plusieurs cartes, il est possible de ne conserver qu'une carte en révoquant les autres. Là aussi, l'annuaire centralisé du GHT permet d'associer la carte à l'identifiant principal de niveau GHT.

**Attribuer aux nouveaux arrivants une carte de niveau GHT, tout en maintenant l'existant pour les autres professionnels.**

Les nouveaux arrivants sont dotés d'une carte rattachée au FINESS juridique de l'établissement support.

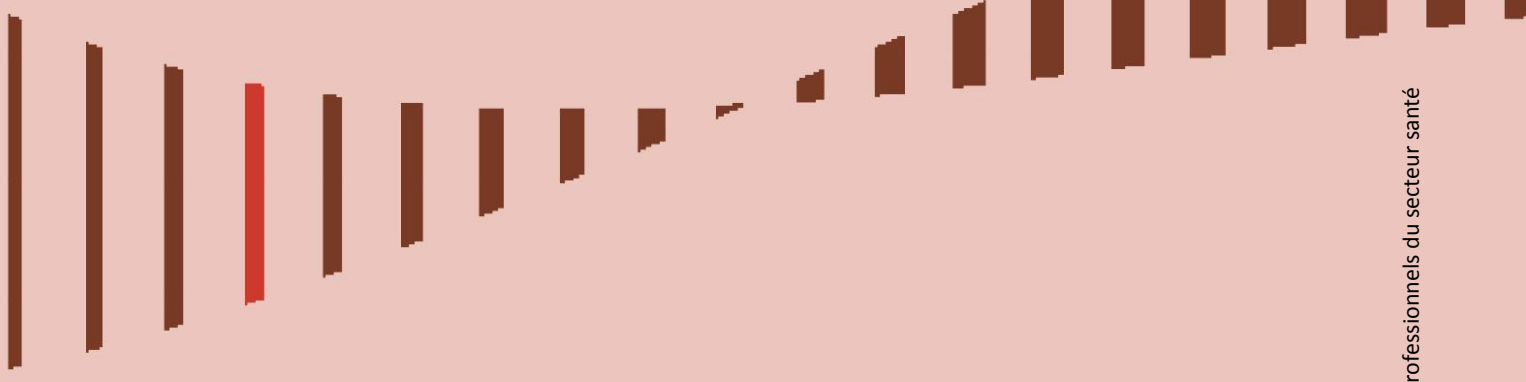
Les cartes des professionnels déjà dotés ne sont pas remises en cause.

**Migration progressive des cartes CPE vers un rattachement à l'établissement support**

Les cartes existantes sont progressivement remplacées par des cartes rattachées au FINESS juridique de l'établissement support.

Pour chaque acteur concerné, une carte CPE rattachée à l'établissement support est commandée, puis sa carte CPE existante est mise en opposition.

Lorsque le GHT dispose d'un nombre significatif de cartes CPE, cette migration doit être assurée en concertation avec l'ASIP Santé en termes de planning.



**L'AGENCE  
FRANÇAISE  
DE LA SANTÉ  
NUMÉRIQUE**

Agence des Systèmes d'Information Partagés de Santé  
9, rue Georges Pitard  
Standard : 01 58 45 32 50  
*Du lundi au vendredi (hors jours fériés)  
de 8h30 à 13h et de 14h à 17h*  
[esante.gouv.fr](http://esante.gouv.fr)