



**MINISTÈRE  
DE LA SANTÉ  
ET DE LA PRÉVENTION**

*Liberté  
Égalité  
Fraternité*

**Direction générale  
de l'offre de soins**

# **Mémento**

## **Dans quel logiciel gérer les identités numériques ? (création, modification des traits, changement de statut...)**

## SOMMAIRE

---

1	Contexte de cette fiche.....	3
2	Rappels .....	3
3	Gestion des identités dans les applicatifs d'un même DI.....	4
3.1	Scénario cible	4
3.2	Scénario toléré	4
4	Mise en œuvre dans les structures de santé .....	5
4.1	Définir le logiciel considéré comme étant le « RI unique »	5
4.2	Identifier et gérer les risques organisationnels	5
4.2.1	Impacts potentiels de la mise en place du scénario cible.....	5
4.2.2	Impacts communs aux 2 scénarios .....	5
5	Synthèse.....	6

## Liste des contributeurs

---

- Mme Ségolène BARD, CRIV GRADeS GE (Pulsy)
- Mme Elsa CREAC'H (ANS)
- Mme Céline DESCAMPS, CRIV GRADeS NA (ESEA)
- M. Thierry DUBREU, GRADeS IdF (SESAN)
- Mme Armelle GONZALEZ, GRADeS BFC
- Mme Soizick GOUY, GRADeS PdL
- Dr Christine LECLERCQ, GIP e-santé Occitanie
- Mme Corinne MIGOT, EFS
- Mme Louisa MILIA, GRADeS Martinique
- Dr Manuela OLIVER, GRADeS PACA (IeSS)
- Mr Loic PANISSE, GIP e-santé Occitanie
- Mme Nathalie PERREAUD, CRIV GRADeS NA (ESEA)
- Dr Bernard TABUTEAU, 3RIV

## 1 CONTEXTE DE CETTE FICHE

L'utilisation d'un référentiel d'identités (RI) unique au sein d'un même domaine d'identification permet de garantir la cohérence des données d'identité dans l'ensemble des logiciels métiers partageant les informations nominatives des usagers pris en charge, et œuvre ainsi en faveur d'une sécurisation de l'identité numérique. Cette garantie n'est cependant réellement obtenue que si la gestion des identités (création, modification, attribution d'un niveau de confiance, appel au téléservice INSi...) est réalisée uniquement dans le RI.

Or, en pratique, les modalités de gestion des identités numériques ont été définies pour s'adapter à des organisations métier existantes. Ainsi, selon le moment et le lieu de la prise en charge, les identités peuvent être créées, modifiées, validées dans des outils différents au sein d'un même domaine d'identification (DI) <sup>1</sup>:

- la gestion administrative du malade (GAM) ou du patient (GAP) si l'accueil était réalisé au bureau des entrées ;
- le dossier patient/usager informatisé (DPI, DUI), général ou spécifique (comme le logiciel des urgences par exemple) si l'accueil était réalisé par un soignant (cas des urgences, de la psychiatrie par exemple) ou d'autres professionnels (laboratoire de biologie, cabinet de radiologie, structure médicosociale par exemple).

Selon le niveau et la qualité de l'interopérabilité mise en œuvre (connexion bidirectionnelle ou non, erreur d'intégration...), l'identité peut alors être différente dans les outils d'un même domaine d'identification (DI). L'objectif final de l'utilisation d'un RI unique, la sécurisation de la prise en charge de l'utilisateur, n'est alors pas atteint.

L'utilisation de l'identité nationale de santé (INS), le respect des exigences et recommandations opposables du Référentiel national d'identitovigilance (RNIV) et du Guide d'implémentation de l'INS (documents à retrouver sur le [site de l'ANS](#)) nécessitent de préciser la gestion des identités dans les outils appartenant à un même domaine d'identification.

***Précision sémantique*** : dans la suite de ce mémento, le terme « identité » sera systématiquement employé pour désigner l'identité numérique de l'utilisateur.

## 2 RAPPELS

On appelle *Référentiel d'identités* (ou RI) tout logiciel qui permet la création/modification des identités. Tout RI doit être notamment capable de créer l'identité d'un usager, de lui attribuer un statut, de la modifier et d'appeler le téléservice INSi<sup>2</sup> afin de récupérer son INS ou de vérifier celle qui a été transmise par un tiers. Ce RI alimente en identité les logiciels métiers du domaine d'identification.

Toute structure sanitaire doit cibler la mise en œuvre d'un seul RI<sup>3</sup> (appelé « **RI unique** » dans la suite du document). **Le RI peut être porté par la GAM/GAP ou le DPI/DUI.**

---

<sup>1</sup> Un domaine d'identification (DI) regroupe au sein d'une organisation de santé toutes les applications qui utilisent le même identifiant pour désigner un patient/usager

<sup>2</sup> Cf. Guide d'implémentation INS

<sup>3</sup> Cf. § 4.2.1 RNIV 1

*Remarque* : un groupe d'établissements peut mettre en œuvre un RI de groupe ; c'est par exemple le cas dans un groupement hospitalier de territoire (GHT). Cette décision doit être prise au niveau du groupe dès que celui-ci s'engage dans la convergence de ses différents systèmes d'information (SI)<sup>4</sup>.

### 3 GESTION DES IDENTITES DANS LES APPLICATIFS D'UN MEME DI

#### 3.1 Scénario cible

L'entière gestion de l'identité : création, modification, appel au téléservice INSi, attribution d'un statut ou d'un attribut, doit être réalisée au sein du RI unique.

Pour rappel : par modification, on entend ici la modification des traits relatifs à l'INS (matricule INS et son OID, nom de naissance, liste des prénoms de naissance, date de naissance, sexe et code lieu de naissance) ainsi que des champs premier prénom de naissance, nom utilisé et prénom utilisé. Ces traits ne doivent pas être modifiés dans un logiciel autre que le RI. En revanche, les autres informations (adresse, coordonnées téléphoniques, médecin traitant, par exemple) peuvent être modifiées dans les autres logiciels. Leur transmission au RI dépend des choix qui ont été faits en termes de mutualisation des informations entre logiciels (décrits dans la cartographie des flux applicatifs de la structure).

Lorsque des identités doivent être créées/modifiées/validées/qualifiées dans des points d'accueil décentralisés, l'établissement doit mettre en place une organisation adaptée :

- soit en mettant en œuvre un logiciel métier ayant le rôle de RI, qui permet de réaliser l'ensemble de la gestion des identités, y compris l'appel au téléservice INSi et le traitement des doublons/collisions ;
- soit en permettant aux agents d'accéder au RI unique et d'y gérer les identités.

Dans ce scénario, le logiciel « RI unique » sera légitime à bloquer tout flux de création / modification d'identités en provenance d'un autre logiciel.

#### 3.2 Scénario toléré

Lorsque l'atteinte du scénario cible n'est pas possible (à court ou moyen terme), il reste toléré de **permettre la création d'une identité, au statut *Identité provisoire***, dans un logiciel autre que le logiciel « RI unique ». Les autres actions (validation de l'identité, modification, qualification...) ne doivent pas être possibles dans ces autres logiciels.

La modification des traits complémentaires (hors nom et prénom utilisé) est possible (médecin traitant, personne de confiance, adresse, n° de tél...).

Dans ce scénario, le logiciel « RI unique » sera légitime à :

- bloquer tout flux de modification d'identités en provenance d'un autre logiciel ;
- intégrer tout flux de création d'une identité au statut *Identité provisoire*<sup>5</sup>.

*A noter* : l'appel au téléservice INSi pour réaliser une opération de vérification de l'INS est possible à

---

<sup>4</sup> Il ne faudrait pas que qu'un établissement considère que la GAM du groupe est le RI unique (maître) alors qu'un autre décide que c'est DPI du groupe...

<sup>5</sup> Quel que soit le statut de l'identité transmis dans le flux, l'identité sera intégrée dans le RI avec un statut provisoire.

partir de tout logiciel et n'est pas réservé au logiciel RI, contrairement à l'opération de récupération de l'INS. En effet tout logiciel qui intègre des données de santé référencées avec l'INS en provenance d'un autre domaine d'identification est censé pouvoir effectuer une vérification de cette INS à réception de ces données.

## 4 MISE EN ŒUVRE DANS LES STRUCTURES DE SANTE

### 4.1 Définir le logiciel considéré comme étant le « RI unique »

L'établissement – ou le groupe d'établissements mettant en œuvre un RI unique commun – doit prendre en compte l'ensemble des impacts organisationnels pour les équipes, tout en sécurisant le processus d'identification primaire pour définir le scénario à appliquer (scénario cible vs scénario dégradé ci-dessus).

### 4.2 Identifier et gérer les risques organisationnels

#### 4.2.1 Impacts potentiels de la mise en place du scénario cible

Si nécessaire :

- former les professionnels des accueils décentralisés à l'utilisation de deux logiciels différents (le RI pour la gestion des identités et le logiciel « métier » pour l'enregistrement des actes, des séjours par exemple) ;
- acquérir les licences supplémentaires nécessaires pour accéder au téléservice INSi, selon les éditeurs (si le coût est calculé à la licence nominative)<sup>6</sup>.

#### 4.2.2 Impacts communs aux 2 scénarios

- Définir la matrice d'habilitation : quels profils/services sont habilités à appeler le téléservice INSi ?
- Mettre à disposition un outil de numérisation des titres d'identité à haut niveau de confiance afin de permettre la conservation du document et de faciliter si besoin le traitement de l'identité en back office.
- Mettre en place une organisation adaptée et un circuit de l'information permettant de reprendre les identités en *back office*, si nécessaire, afin de leur attribuer le bon niveau de confiance après appel du téléservice INSi.

---

<sup>6</sup> Le 3RIV identifie un risque d'utilisation de login générique pour diminuer les coûts et attirent l'attention des professionnels/structures sur l'interdiction d'utiliser des logins génériques pour gérer les identités (cf. exigences de traçabilité).

## 5 SYNTHÈSE

- Une structure doit avoir un RI unique.
- Un groupe de structures peut faire le choix de mettre en œuvre un RI unique commun.
- Le RI peut être la GAM/GAP, le DPI ou le DUI de la structure ou du groupe de structures.
- Le RI est le seul outil légitime servant à gérer l'ensemble des identités du domaine d'identification (création, modification, attribution d'un statut, récupération de l'INS par le téléservice INSi).
- La création d'une identité dans un autre outil est possible mais uniquement au statut *Identité provisoire*, avant d'être transmise au RI.
- La modification de l'identité hors RI est possible au niveau des traits complémentaires, hormis sur les champs *Nom utilisé* et *Prénom utilisé*.