MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Référentiel national d'identitovigilance

1. Principes d'identification des usagers communs à tous les acteurs de santé

Statut : Validé | Classification : Public | Version v1.2

SOMMAIRE

Contributeurs

M. Raphaël BEAUFFRET, DNS

Mme Christelle BOULIN, ANS

M. Bruno CHAMPION, DGS

Mme Elsa CREACH, ANS

Mme Céline DESCAMPS, CRIV NA

M. Thierry DEZERCES, ARS Ile de France

M. Thierry DUBREU, GRADeS IDF (SESAN)

M. Marc FUMEY (HAS)

Dr Gilles HEBBRECHT, DGOS

Dr Christine LECLERCQ, GRADeS Occitanie (e-santé Occitanie)

Mme Bérénice LE COUSTUMER, DGOS

M. Mikaël LE MOAL, DGOS

Dr Isabelle MARECHAL, CHU Rouen

Mme Christelle NOZIERE, CRIV NA

Dr Manuela OLIVER, GRADeS PACA (ieSS)

M. Loïc PANISSE, GRADeS Occitanie (e-santé Occitanie)

Mme Emilie PASSEMARD (DNS)

M. Bertrand PINEAU, GRADeS IDF (SESAN)

Mme Isabelle STACH, GRADeS Occitanie (e-santé Occitanie)

M. Michel RAUX, DGOS

Dr Bernard TABUTEAU, CRIV NA

Mme Charlotte VOEGTLIN, GCS Tesis, La Réunion

L'équipe remercie les différents professionnels qui ont contribué à améliorer ce document lors de la phase de concertation.

Historique des versions

Version	Date	Contexte
1.0	30/10/2020	1ère mise en ligne du document
1.1	20/12/2020	Correction de coquilles et ajustements mineurs de contenu
1.2	20/05/2021	Mise à jour, notamment suite avis CNIL

1 Introduction

1.1 Enjeux de l'identification des usagers de la santé

La bonne identification d'un usager est un facteur clé de la sécurité de son parcours de santé. Elle constitue le premier acte d'un processus qui se prolonge tout au long de sa prise en charge par les différents professionnels de la santé impliqués, quels que soient la spécialité, le secteur d'activité et les modalités de prise en charge.

Un grand nombre d'acteurs (professionnels de santé comme usagers) semblent pourtant méconnaître les risques encourus en cas d'identification imparfaite. L'événement indésirable le plus fréquent est l'administration de soins au mauvais patient. Mais la mauvaise identification peut aussi être source (liste non exhaustive) : de retard de prise en charge, d'erreur diagnostique, d'erreur thérapeutique, d'échange d'informations erronées entre professionnels, d'enregistrement de données de santé dans un dossier qui n'est pas celui de l'usager concerné (collision), de création de plusieurs dossiers pour un même usager (doublons), d'erreur de facturation…

Le processus d'identification est également un des éléments socles pour le déploiement des politiques nationales de santé et notamment de la feuille de route du numérique en santé[1]. Il est indispensable qu'un usager soit identifié de la même façon par tous les professionnels qui partagent des données de santé qui le concernent. L'obligation de référencement par l'*identifiant national de santé* (INS) à partir du 1er janvier 2021 est une des réponses à cet enjeu. Elle nécessite la mise en place de bonnes pratiques, respectées par l'ensemble des acteurs, pour éviter de propager un matricule INS incorrectement associé à une identité numérique.

Élément de confiance dans les échanges de données de santé, la bonne identification représente un enjeu national majeur pour la sécurité des soins. La vérification de l'identité fait intégralement partie de l'acte de soin ; elle est réalisée sous la responsabilité du professionnel de santé assurant la prise en charge. La participation de l'usager (ou à défaut celle de ses proches), acteur de sa propre sécurité, doit être recherchée chaque fois que possible pour faciliter cette étape ; en dehors des situations réglementaires d'anonymat de prise en charge, l'usager ne peut s'opposer à la vérification de son identité par un professionnel de santé.

La responsabilité des acteurs de santé et des dirigeants de structures pourrait être mise en cause s'il s'avérait que le défaut de mise en œuvre des bonnes pratiques d'identification était à l'origine d'un dommage ou de la mise en danger d'un usager.

1.2 Référentiel national d'identitovigilance

Le référentiel national d'identitovigilance (RNIV) a pour objet de fixer les exigences et recommandations à respecter en termes d'identification des usagers pris en charge sur le plan sanitaire ou médico-social par les différents professionnels impliqués (structures de ville, établissements de santé, secteur médico-social, acteurs sociaux) afin de maîtriser les risques dans ce domaine.

Remarque : Le RNIV n'évoque pas la question de l'identité nécessaire à la facturation des soins : l'Assurance maladie utilise des traits d'identification qui peuvent avoir des différences notables

[1] https://esante.gouv.fr

avec l'identité officielle mais qui ne sont pas pris en compte dans le domaine de l'identitovigilance.

Le RNIV est annexé au référentiel « Identifiant national de santé », qu'il vient compléter. A ce titre, il est opposable à tous les acteurs qui concourent à cette prise en charge en traitant des données de santé : usagers, professionnels de santé, agents chargés d'assurer la création et la modification des identités dans le système d'information, mais aussi éditeurs informatiques, responsables de traitement de l'ensemble des applications e-santé[2], Assurance maladie (en tant que gestionnaire du dossier médical partagé et maître d'œuvre du téléservice INSi) voire organismes complémentaires (offres de services relatifs aux soins) et services sociaux (lorsqu'ils participent à la prise en charge).

Le RNIV se substitue aux documents établissant des règles d'identitovigilance régionales (référentiel ou charte). Il fixe le niveau minimal de sécurité que toutes les parties prenantes doivent appliquer pour l'identification des usagers. Les exigences et recommandations peuvent toutefois être complétées ou précisées par des documents pratiques ou des consignes particulières relevant des instances nationales, régionales, territoriales et/ou locales.

Remarque :

Le RNIV se compose actuellement de 5 volets :

0- Recueil des points essentiels

1- Principes d'identification des usagers communs à tous les acteurs de santé

2- Mise en œuvre de l'identitovigilance dans les établissements de santé

3- Mise en œuvre de l'identitovigilance dans les structures non hospitalières

4. Mise en œuvre de l'identitovigilance par les acteurs libéraux

[2] Sans oublier le dossier médical partagé (DMP), le dossier pharmaceutique (DP), etc.

2 Définitions

2.1 Identité, identification, identitovigilance

L'identité est l'ensemble des *traits* ou caractéristiques qui permettent de reconnaître une personne physique et d'établir son individualité au regard de la loi (date et lieu de naissance, nom, prénom, filiation, etc.). Ces éléments sont attestés par des documents officiels d'état civil ou leur équivalent numérique.

L'identification correspond aux opérations permettant d'établir l'identité d'un individu au regard de l'état-civil, de le reconnaître comme individu physique, de lui créer un dossier personnel papier et/ou numérique. En santé, on distingue 2 domaines complémentaires dans l'identification des usagers :

- *l'identification primaire* : elle comprend l'ensemble des opérations destinées à attribuer à un usager physique, de manière univoque, une identité numérique qui lui est propre dans un système d'information de santé, qu'il s'agisse d'une première prise de contact avec l'usager ou d'une venue ultérieure ; elle recouvre les étapes de recherche, de création, de modification d'une identité ainsi que l'attribution d'un niveau de confiance aux données enregistrées (cf. 3.3) ;
- *l'identification secondaire* : elle correspond aux moyens mis en œuvre, à l'occasion de la prise en charge d'un usager physique (soin, administration médicamenteuse, prélèvement biologique, examen d'imagerie médicale, etc.), pour s'assurer que le bon soin sera délivré au bon patient ; elle consiste notamment à vérifier, à chaque étape de sa prise en charge, l'adéquation entre son identité réelle et celle présente sur les documents et outils de prise en charge (dossier physique ou informatique, prescription, étiquette, bon de transport, compte-rendu d'examen, etc.).

L'identité numérique correspond à la représentation d'un individu physique dans un système d'information (cf. Annexe I). Un même usager physique est ainsi associé à plusieurs identités numériques selon le système d'information utilisé : employeur, impôts, sécurité sociale, mutuelle, banque, etc.

L'*identitovigilance* est définie comme l'organisation mise en œuvre pour fiabiliser l'identification de l'usager et sécuriser ses données de santé, à toutes les étapes de sa prise en charge. Elle concerne la compréhension et le respect par tous les acteurs des règles d'identification ainsi que la gestion des risques liés aux erreurs rencontrées. Elle fait intégralement partie de la sécurisation des données qui incombe au responsable de traitement de l'identité : personne morale, professionnel libéral, directeur d'établissement, gestionnaire d'application e-santé…

2.2 Identité nationale de santé

L'*identité nationale de santé* (INS) est une identité numérique qui repose sur des bases nationales de référence (cf. 3.2). Le RNIV utilise le terme d'*identité INS* pour évoquer l'ensemble des informations qui le composent. Chaque identité INS comprend les éléments suivants :

- le *matricule INS* qui a pour valeur le NIR (ou le NIA) personnel de l'usager, sur 15 caractères ;
- les *traits INS* qui sont les traits d'identité de référence associés au NIR/NIA dans les bases de référence (nom de naissance, prénom(s), sexe, date de naissance et code INSEE du lieu de naissance) ;

- l'organisme qui a affecté l'INS, précisé sous la forme d'un *OID* (*object identifier*), information habituellement invisible pour le professionnel de santé (le NIR et le NIA ayant chacun leur autorité d'affectation, cela permet de les distinguer).

Exemple fictif d'une identité INS

Matricule INS	*Nom*	*Prénom(s)*	*Sexe*	*DDN*	*Lieu nais.*	*OID*
260058815400233	*DARK*	*JEANNE MARIE CECILE*	*F*	*30/05/1960*	*88154*	*1.2.250.1.213.1.4.8*

2.3 Conventions sémantiques

Dans le RNIV, les termes *acteur de santé* et *structure de santé* sont utilisés de façon générique pour identifier les professionnels (administratifs et soignants) et entités dans lesquelles ils interviennent : cabinet médical, structure hospitalière, établissement médico-social, service social, plateforme de coordination des soins, etc.

La notion de *nom de famille* étant très souvent confondue avec celle de *nom d'usage*, il a été fait le choix de retenir l'appellation *nom de naissance* dans le RNIV en substitution de *nom de famille*.

Le RNIV introduit également les notions de *nom utilisé* et de *prénom utilisé* qui diffèrent, dans leur finalité, du *nom d'usage* et du *prénom usuel* dont la définition est liée à l'état civil (cf. Annexe II).

Les exigences (« Exi ») et recommandations (« Reco ») sont signalées en gras dans le texte et compilées en Annexe III ; elles concernent le système d'information (SI) et/ou les pratiques professionnelles (PP).

La ressemblance entre certains vocables pouvant prêter à confusion, le RNIV utilise par convention les termes :

- *contrôle/contrôler* pour toutes les opérations d'évaluation de cohérence entre plusieurs jeux de traits ;
- *qualification/qualifier* à l'attribution du statut *Identité qualifiée* de l'identité numérique ;
- *récupération/récupérer* aux opérations de recherche et récupération de l'identité INS ;
- *validation/valider* à l'attribution du statut *Identité validée* de l'identité numérique ;
- *vérification/vérifier* aux opérations de vérification de l'identité INS.

3 Bonnes pratiques pour l'identification primaire d'un usager

Les règles générales décrites dans ce chapitre concernent la gestion de l'identité numérique de l'usager dans les systèmes d'information de santé (SIS).

3.1 Règles générales concernant l'enregistrement numérique d'un usager

3.1.1 Comment rechercher un enregistrement dans la base locale ?

3.1.1.1 Rechercher l'antériorité d'un enregistrement

Pour éviter la création de plusieurs identités numériques pour un même usager (doublons) ou l'intégration de données dans un dossier autre que le sien (collisions), la recherche de l'enregistrement d'un usager dans le référentiel d'identité de la structure est impérative avant toute création d'une identité, selon des modalités définies par chaque structure ou acteur de santé.

Le système d'information doit permettre d'effectuer la recherche d'une identité numérique à partir :

- de tout ou partie de l'identité INS récupérée après l'interrogation du téléservice INSi ;
- de la saisie de la date de naissance, éventuellement complétée par les premiers caractères du nom ou du prénom. [Exi SI 01]

L'utilisation du matricule INS pour la recherche d'antériorité doit être sécurisée pour éviter tout risque lié à une erreur de saisie. Si le matricule n'est pas récupéré électroniquement, la saisie des 15 caractères du NIR et leur validation par la clé de contrôle est obligatoire pour toute recherche à partir du matricule INS. [Exi SI 02]

Pour obtenir des résultats pertinents, il est fortement recommandé de limiter le nombre de caractères saisis pour effectuer la recherche d'un enregistrement à partir du nom ou du prénom. [Reco PP 01]

Exemple : recherche effectuée avec la date de naissance + 3 premiers caractères du nom de naissance.

Remarque : il peut exister des outils performants pour effectuer la recherche d'antériorité sur la base d'un taux de ressemblance ou d'une recherche phonétique ; leur utilisation est possible sous réserve que l'éditeur s'engage en termes de sécurité des résultats renvoyés et que la structure de santé en valide la pratique.

Lors de la recherche d'un usager dans la base d'identités, il est nécessaire que le système d'information interroge sans distinction, avec les données correspondantes mais sans tenir compte des tirets ou apostrophes, les champs *Nom de naissance* et *Nom utilisé*, ainsi que les champs *Prénom(s) de naissance, Premier prénom de naissance* et *Prénom utilisé*. [Exi SI 03]

3.1.1.2 Affichage des résultats de la recherche

Les résultats de la recherche doivent être affichés de façon suffisamment informative pour que le professionnel puisse déterminer sans risque d'erreur s'il peut sélectionner le dossier correspondant à l'usager pris en charge ou s'il doit créer une nouvelle identité numérique.

L'affichage doit comporter *a minima* les traits stricts (cf. 3.1.3.1)[3] et, si applicable, les dates des dernières venues. Lorsque c'est possible, il doit aussi signaler les informations relatives au statut de l'identité et aux attributs éventuellement associés (cf. 3.3).

3.1.2 Comment créer une identité numérique ?

Plusieurs possibilités existent pour enregistrer un nouvel usager dans le système d'information de la structure. L'identité numérique peut être créée :

- à partir des traits INS récupérés automatiquement après interrogation du téléservice INSi (cf. 3.1.2.1) ;
- par la saisie manuelle de traits d'identité fournis directement par l'usager ou un accompagnant (cf. 3.1.2.2) ;
- à partir de l'identité numérique transmise par une autre structure ayant pris en charge l'usager ou par le patient lui-même par le biais d'outils adaptés (hors interrogation du téléservice, cf. 3.1.2.3) ;
- à partir de traits fictifs ou approximatifs dans le cadre de l'accueil d'un usager difficile à identifier ou bénéficiant d'un dispositif d'anonymat (cf. 3.1.2.4).

3.1.2.1 Récupération de l'identité INS

Il est possible d'interroger le téléservice INSi via le système d'information de santé, soit par utilisation de la carte Vitale de l'usager ou de son ouvrant droit (cf. 3.2.1.2), soit par saisie des traits de l'identité numérique locale (cf. 3.2.1.3).

3.1.2.2 Saisie manuelle des traits d'identité

La qualité de l'identité numérique enregistrée dépend des modalités d'enregistrement de celle-ci, selon que l'identité est recueillie :

- à partir d'un document preuve, selon le type de document présenté (cf. 3.3.3.2) ;
- à l'aide d'informations données de façon orale par l'usager, un proche ou tout autre intermédiaire ;
- dans des conditions très dégradées (usager non accompagné inconscient, confus, non francophone…).

Lorsqu'une pièce d'identité est présentée, les traits doivent être enregistrés tels qu'ils apparaissent sur le document fourni (cf. 3.1.2.4) mais en respectant les règles de saisies définies dans le présent référentiel : des consignes particulières sont données en Annexe IV pour l'enregistrement de certains traits.

3.1.2.3 Utilisation d'une identité transmise à partir d'un domaine d'identification différent

Dans certains cas, l'enregistrement d'un usager se fait sans qu'il soit physiquement présent. C'est le cas, par exemple :

- pour un prestataire qui réalise un acte à distance (laboratoire, télémédecine) ;
- pour un professionnel qui reçoit des données de santé concernant un usager non enregistré dans le système d'information qu'il utilise ;

[3] **La pertinence de faire apparaitre le matricule INS sur les résultats des écrans de recherche ainsi que le nom et prénom utilisés est à arbitrer par la structure**

- lors de procédures qui permettent à l'usager de s'enregistrer en ligne (solutions amont de prise de rendez-vous/pré-consultation/pré-admission au sein d'un portail patient en ligne) ;
- lorsque l'identité est reçue sous format papier (cf. 4.2.3.2).

Les traits transmis sans matricule INS doivent être enregistrés par défaut au statut *Identité provisoire*. Ils peuvent cependant être enregistrés au statut *Identité validée* si l'identité de l'usager a été vérifiée sur la base d'un dispositif d'identification électronique certifié substantiel eIDAS(notamment dans le cas d'une prise de rendez-vous / préadmission en ligne par l'intermédiaire d'une solution proposant ce niveau d'identification électronique).

Lorsque l'identité transmise est accompagnée d'un matricule INS, les traits doivent faire l'objet d'une vérification par appel au téléservice INSi qui permet, en cas de conformité, d'enregistrer par défaut l'identité INS au statut *Identité récupérée*. L'identité INS peut cependant être enregistrée au statut *Identité qualifiée* si l'identité de l'usager a été vérifiée sur la base d'un dispositif d'identification électronique certifié substantiel eIDAS (notamment dans le cas d'une prise de rendez-vous / préadmission en ligne par l'intermédiaire d'une solution proposant ce niveau d'identification électronique).

En cas de non-conformité, les traits stricts sont enregistrés au statut *Identité provisoire*, sans conserver le matricule INS.

L'appel au téléservice INSi est obligatoire pour vérifier une identité INS reçue lorsque l'identité numérique n'existe pas ou qu'elle ne dispose pas d'un statut récupéré ou qualifié. [Exi PP 01]

Lorsque cette identité n'est pas transmise par voie informatique mais doit être recopiée manuellement, il est possible de faire appel à l'opération de recherche par saisie des traits afin de faciliter et sécuriser la récupération des traits et du matricule INS (cf. 3.2.1.3 et 4.2.3.2).

L'Annexe V développe des exemples de cas d'usages relatifs à l'identification des usagers à distance (inscription à distance, sous-traitance, télémédecine, télé-expertise…) et précise les conditions dérogatoires concernant les prestataires de service liés par contrat à des structures qui leur sous-traitent des actes.

3.1.2.4 Création d'une identité fictive ou approximative

Il existe des situations où il n'est pas possible d'identifier un usager avec sa véritable identité :
- accueil d'un usager non accompagné non communiquant ou délirant ;
- accueil massif de victimes en situation sanitaire exceptionnelle ;
- usager faisant valoir son droit à une prise en charge anonyme.

Comme la création d'une identité numérique est obligatoire pour enregistrer la prise en charge, celle-ci fait appel à des traits fictifs ou approximatifs qui seront, si possible, corrigés secondairement. Les acteurs concernés doivent mettre en œuvre une procédure *ad hoc* qui définit les modalités de gestion des 5 traits stricts obligatoires à renseigner (cf. 3.1.3.1) en fonction des éléments pouvant être recueillis (cf. Annexe IV). L'identité numérique doit être associée à l'attribut *Identité douteuse* ou *Identité fictive* (cf. 3.3.2).

3.1.3 Quelles sont les informations à recueillir ?

La bonne identification d'un usager nécessite l'enregistrement d'un certain nombre d'informations, appelées « traits », dont l'importance est variable.

Les traits d'identification doivent faire l'objet de champs spécifiques dans le système d'information. [Exi SI 04]

3.1.3.1 Les traits invariables (traits stricts)

Ce sont les traits de référence qui servent à établir l'identité officielle d'une personne physique, sans risque d'erreur. Les traits stricts comprennent :

- le nom de naissance (nom de famille) ;
- le premier prénom de naissance[4] ;
- la date de naissance ;
- le sexe ;
- le lieu de naissance (code INSEE de la commune de naissance pour les personnes nées en France ou du pays de naissance pour les autres) ;
- la liste des prénoms de naissance ;
- le matricule INS (complété par son *OID*, cf. 2.2)[5].

La création d'une identité numérique requiert la saisie d'une information dans au moins 5 traits stricts : nom de naissance, premier prénom de naissance, date de naissance, sexe et lieu de naissance. [Exi PP 02]

Les champs relatifs à la liste des prénoms de naissance et au matricule INS sont renseignés dès qu'il est possible d'accéder à ces informations : présentation d'un titre d'identité et/ou appel au téléservice INSi (dans les cas d'usage où sa recherche est requise et autorisée). [Exi PP 03]

Exemple (fictif) :

L'identité officielle de Mme Jeanne Marie Cécile DARK veuve LOUIS est composée des traits de référence de son identité INS, sans l'*OID* (cf. exemple du § 2.2) :

Nom	*Prénom(s)*	*Sexe*	*DDN*	*Lieu nais.*	*Matricule INS*
DARK	*JEANNE MARIE CECILE*	*F*	*30/05/1960*	*88154*	*260058815400233*

Son premier prénom est JEANNE.

Les règles d'enregistrement manuel de ces traits sont précisées en Annexe IV.

3.1.3.2 Autres traits (traits complémentaires)

Ce sont des informations personnelles qui complètent les traits stricts d'un usager. Elles ne servent pas à établir son identité officielle mais sont essentielles pour faciliter certaines opérations relatives à la prise en charge de l'usager ou à des traitements relatifs à la gestion des risques (cf. 4).

Enregistrés dans des champs dédiés, ils comprennent (liste non limitative) :

- nom et le prénom utilisés dans la vie courante ;
- code postal et/ou nom de la commune de naissance (cf. Annexe IV) ;
- adresse postale de l'usager ;

---

[4] Champ conservé pour assurer la compatibilité entre logiciels, cf. modalités de saisie en Annexe 1

[5] Cf. référentiel INS (https://esante.gouv.fr/sites/default/files/media_entity/documents/ASIP_R%C3%A9f%C3%A9rentiel_Identifiant_National_de_Sant%C3%A9_v1.pdf)

- numéros de téléphone de l'usager ou de son tuteur ;
- adresse mail de l'usager ou de son tuteur ;
- photographie[6] ;
- profession ;
- numéro de sécurité sociale de l'ouvrant droit (il concerne les différents ayants droit d'un seul assuré) ;
- identités et coordonnées des personnes en relation (parent, enfant, conjoint, personne de confiance…) ;
- numéro de téléphone ou l'adresse mail de l'ouvrant droit ;
- coordonnées du médecin traitant ;
- autres professionnels de santé impliqués dans la prise en charge ;
- nature du document d'identité présenté ;
- etc.

Le système d'information doit permettre la saisie des traits complémentaires *Nom utilisé* et *Prénom utilisé*. [Exi SI 05]

Il est nécessaire de renseigner le maximum de traits complémentaires, selon les consignes que chaque structure définit en fonction de ses besoins. [Exi PP 04]

3.1.3.3 Précisions sémantiques

Les champs *nom utilisé* et *prénom utilisé* sont des champs nouveaux, introduits par le RNIV pour recueillir l'identité utilisée par l'usager dans la vie courante. Ils ont pour objet de faciliter le dialogue soignant-soigné, notamment dans les situations de contrôles de cohérence relatives à l'identification secondaire (avant chaque acte), le but étant de renforcer la relation de confiance professionnel-patient et de faciliter le travail et le suivi par le professionnel de son patient.

Les modalités de recueil de ces champs sont précisées en Annexe IV.

Exemple :
Mme JEANNE, MARIE, CECILE, DARK veuve LOUIS, a toujours utilisé son nom de naissance dans la vie courante bien que son nom d'usage, LOUIS, soit précisé sur sa carte d'identité et qu'elle tienne à ce que cette mention perdure. De même, bien que cela ne soit pas conforme aux règles d'état civil, elle utilise depuis son plus jeune âge le prénom composé Marie-Cécile sans l'avoir jamais fait officialiser.

Il est préconisé d'inscrire DARK comme *nom utilisé* et MARIE-CECILE comme *prénom utilisé* afin qu'elle puisse continuer d'être appelée par ces traits lors des contacts qu'elle entretient avec les acteurs de santé.

Remarque : le nom de son mari décédé, jamais utilisé, ne figure pas dans les traits complémentaires mais peut faire l'objet, si besoin, d'un enregistrement dans un champ « Autre », s'il existe, selon les arbitrages locaux formalisés dans une procédure *ad hoc*.

Chaque structure ou acteur de santé, en fonction de ses activités, de sa patientèle, définit localement des règles d'alimentation de ces champs. Le choix peut être fait de ne prendre en compte que le nom d'usage et le prénom usuel (au sens de l'état civil), mentionné(s) sur une pièce d'identité ou d'alimenter ces champs, comme dans l'exemple ci-dessus, par le nom et le prénom

[6] Sous réserve du respect du droit à l'image et des règles de conservation des données en vigueur

réellement utilisés dans la vie courante. Cette décision doit être tracée, formalisée, communiquée.

3.2 Règles générales concernant l'emploi de l'identité INS

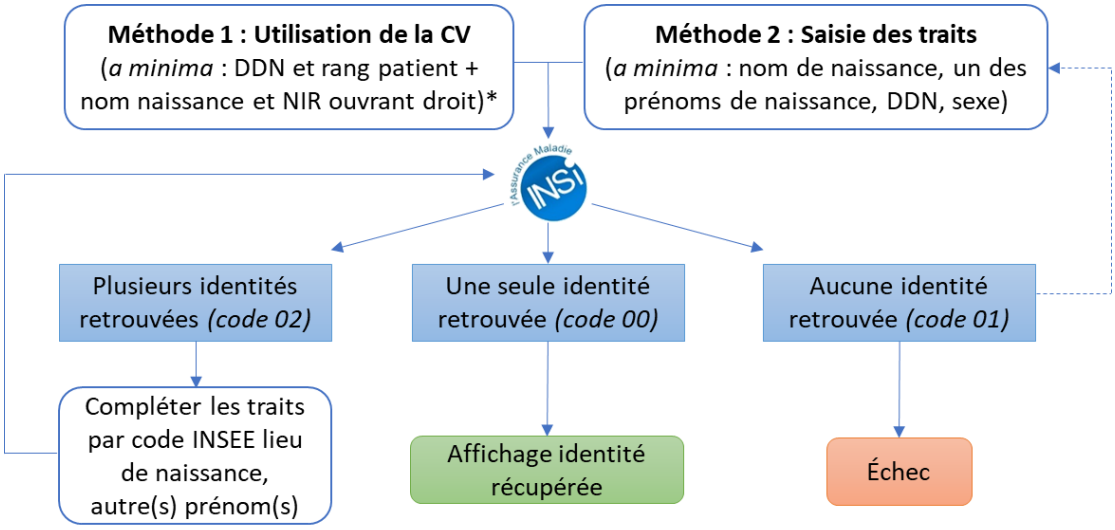
3.2.1 Comment récupérer et gérer l'identité INS ?

3.2.1.1 Généralités

L'identité INS de l'usager est recherchée, récupérée et/ou vérifiée par appel à un téléservice dédié nommé INSi[7]. Quand il est requis, l'appel à ce téléservice se fait par l'intermédiaire du système d'information en santé (SIS) et sous couvert d'une authentification de l'utilisateur (exemple : carte CPx physique ou procédure d'authentification dématérialisée).

L'interrogation du téléservice peut se faire selon 2 modalités :

- par l'intermédiaire de la carte Vitale (cf. 3.2.1.2)[8] ;
- par saisie des traits d'identité enregistrés localement ou transmis par un tiers (cf. 3.2.1.3).



Les informations récupérées du téléservice INSi font l'objet d'un stockage et d'une traçabilité au niveau du système d'information de santé. [Exi SI 06]

Remarque : pour certains usagers, la base de référence de l'identité INS contient des valeurs vides (ou nulles) dans les champs nom, prénom(s), sexe et/ou certaines parties de la date de naissance (00/00/AAAA, 00/MM/AAAA ou JJ/00/AAAA). Ces données étant incompatibles avec les règles du RNIV, l'identité INS de ces usagers ne peut pas être acceptée (cf. Annexe VI). Leur identité numérique ne doit être renseignée que de façon manuelle (cf. 3.1.2.2) ou à partir d'informations transmises par un tiers (cf. 3.1.2.3), sans possibilité de récupérer l'identité INS.

Avant toute intégration de l'identité INS dans l'identité numérique locale, il est nécessaire de valider la cohérence entre les traits INS renvoyés par le téléservice INSi et les traits de la personne physique prise en charge. [Exi PP 05]

La démarche d'évaluation de la cohérence entre les jeux de traits est précisée en Annexe VI.

---

[7] https://esante.gouv.fr/securite/identifiant-national-de-sante

[8] Actuellement, le téléservice INSi interdit l'utilisation de l'empreinte de la carte Vitale

Remarque : hors cadre réglementaire de l'anonymat, l'usager ne peut s'opposer à l'utilisation de l'identité INS mais doit en être informé[9] ainsi que de son droit d'accès et de rectification des données.

3.2.1.2 Opération de recherche par utilisation de la carte Vitale

L'interrogation du téléservice INSi par l'intermédiaire de la carte Vitale est le mode d'interrogation à privilégier chaque fois que possible. [Exi PP 06]

La procédure utilise certains traits recueillis par l'intermédiaire de la carte Vitale[10], de façon transparente pour l'utilisateur. Une concordance parfaite doit être trouvée afin de récupérer l'identité INS. Cette recherche peut, dans quelques cas, être infructueuse.

3.2.1.3 Opération de recherche par saisie des traits d'identité

L'interrogation du téléservice par saisie des traits n'est pas recommandée en première intention. Elle ne doit être utilisée que dans les cas où :
- la carte Vitale n'est pas présentée par l'assuré ;
- l'accès par lecture de la carte Vitale n'est pas opérationnel ;
- la recherche par l'intermédiaire de la carte Vitale est infructueuse ;
- l'identité numérique a été transmise par un tiers (cf. 3.1.2.3).

Les traits à utiliser sont, *a minima* : le nom de naissance, un des prénoms de naissance, le sexe, la date de naissance. Une concordance parfaite est attendue au niveau des identités présentes dans la base de l'INSi. Si une seule identité INS est retrouvée dans la base (code « 00 »), le téléservice affiche les traits INS correspondants à l'identité saisie et permet de la récupérer. Dans le cas où plusieurs identités INS sont retrouvées (code « 02 »), le téléservice ne fournit pas de liste ; il sera nécessaire de compléter l'identité par la saisie du lieu de naissance (code officiel géographique INSEE, cf. Annexe IV) voire des autres prénoms de naissance. Cette recherche peut, dans quelques cas, rester infructueuse (code « 01 »).

3.2.1.4 Remarques importantes

L'interrogation du téléservice INSi n'est pas indiquée dans plusieurs situations ; par exemple :
- usager qui n'a aucune raison d'être immatriculé en France (touriste étranger…) ;
- identité considérée comme douteuse ou fictive (cf. 3.3.2) ;
- prise en charge du nouveau-né avant l'attribution d'un NIR (donc également le fœtus *in utero*) ;
- situation d'anonymat légal[11].

3.2.2 Quelles sont les informations renvoyées par le téléservice INSi ?

Parmi les informations contenues dans l'identité INS renvoyée par le téléservice INSi, celles qui permettent l'identification de l'usager sont :
- le *matricule INS*, constitué du numéro d'identification de l'individu au répertoire des personnes physiques (NIR ou NIA) ;

---

[9] Cf. Référentiel INS (https://esante.gouv.fr/sites/default/files/media_entity/documents/ASIP_R%C3%A9f%C3%A9rentiel_Identifiant_National_de_Sant%C3%A9_v1.pdf)

[10] Guide d'intégration du téléservice INSi : http://www.sesam-vitale.fr/documents/20182/75606/SEL-MP-043_01-00_INSi+sans+MR/92d6e408-012d-4dc5-9fd1-d3bdda78735a

[11] Accouchement dans le secret, centre de planification…

- les *traits INS*, traits d'identité provenant de la base nationale de référence (SNGI) :
    - le nom de naissance ;
    - le(s) prénom(s) de naissance (séparés par des espaces) ;
    - la date de naissance ;
    - le sexe ;
    - le code géographique du lieu de naissance.

Remarque : le téléservice INSi peut également renvoyer un « prénom usuel » enregistré dans les bases de données de l'Assurance maladie ; comme ce n'est pas un trait de référence de la base d'état civil, sa récupération par le système d'information doit être ignorée.

3.3 Niveaux de confiance attribués à l'identité numérique locale

L'enregistrement des traits d'identité doit être associé à une information qui précise, en fonction des modalités de recueil et de contrôle de cohérence, le niveau de confiance qu'on peut accorder à l'identité numérique créée, ce qui a des conséquences pour ses usages ultérieurs.

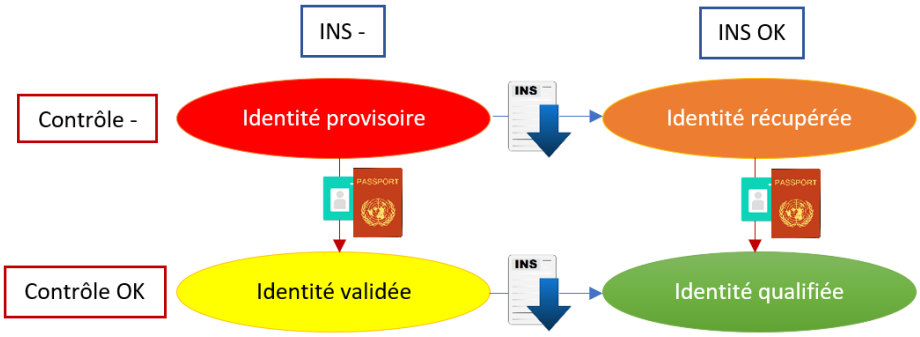
3.3.1 Quels sont les statuts de confiance d'une identité numérique ?

La confiance à accorder à une identité numérique correspond à un couple de déterminants indiquant si les traits de l'identité numérique enregistrée dans le SIS :

- sont issus de l'identité INS récupérée à partir des bases de référence par l'intermédiaire du téléservice INSi [I+] ou non [I-] ;
- ont bénéficié d'un contrôle de cohérence à partir des traits portés par un titre d'identité à haut niveau de confiance ou son équivalent numérique [C+] ou non [C-].

Il est ainsi distingué 4 niveaux croissants de confiance pour l'identité numérique locale :

- le statut ***Identité provisoire*** [I-, C-] est celui qui est attribué, par défaut, à toute identité numérique créée sans utilisation du téléservice INSi ;
- le statut ***Identité récupérée*** [I+, C-] est attribué lorsque l'identité numérique est créée à partir de l'identité INS récupérée après interrogation du téléservice INSi (cf. 3.2.1) ;
- le statut ***Identité validée*** [I-, C+] est attribué après contrôle de cohérence des traits enregistrés en *identité provisoire* avec ceux portés par un dispositif d'identification à haut niveau de confiance (cf. 3.3.3.2) ;
- le statut ***Identité qualifiée*** [I+, C+], qui associe la récupération de l'identité INS (ou sa vérification) à partir du téléservice INSi et le contrôle de cohérence des traits enregistrés avec ceux portés par un dispositif à haut niveau de confiance.



Tout système d'information en santé doit permettre d'attribuer un des 4 statuts de confiance à chaque identité numérique stockée. [Exi SI 07]

L'attribution d'un niveau de confiance à toute identité numérique est obligatoire. [Exi PP 07]

Le statut *identité qualifiée* est le seul à permettre d'utiliser le matricule INS lors des transmissions de données au sein du système d'information de santé (SIS)[12].

Le système d'information doit garantir que seul le statut *Identité qualifiée* permette le référencement des données de santé échangées avec le matricule INS, en conformité avec la réglementation applicable. [Exi SI 08]

L'Annexe VII donne des exemples de situations d'évolution du statut de confiance de l'identité numérique.

3.3.2 Quels sont les attributs complémentaires pouvant être utilisés ?

Il est recommandé que les systèmes d'information en santé autorisent l'emploi d'attributs supplémentaires pour permettre aux professionnels de caractériser les identités numériques nécessitant un traitement particulier. [Reco SI 01]

L'attribut ***Identité homonyme*** a pour objet de faciliter l'identification et la gestion des identités numériques à fort taux de ressemblance (homonymes avérés et identités approchantes) qui doivent faire l'objet d'une vigilance particulière[13] de la part des acteurs de santé. Il peut être associé à chacun des 4 statuts précédemment définis et n'est pas, sauf exception (exemple : modification *a posteriori* d'un des traits stricts), modifié au cours des éventuels changements de statut d'une identité. Cet attribut peut être diffusé à l'ensemble des applications du domaine d'identification.

L'attribut ***Identité douteuse*** permet de tracer l'existence d'un doute sur la véracité de l'identité recueillie (usager confus, suspicion d'utilisation frauduleuse d'identité, situation sanitaire exceptionnelle…). Il ne peut être associé qu'à un statut *Identité provisoire*. Dans le cas où il est associé à une identité numérique ayant précédemment reçu un statut de confiance supérieur, il entraîne la rétrogradation du statut en *Identité provisoire* et, lorsqu'un matricule INS était associé, sa suppression (ou son invalidation).

L'attribut ***Identité fictive*** peut uniquement être associé au statut *Identité provisoire*. Il a pour objet de faciliter la gestion :

- des identités dites sensibles, faisant l'objet d'une règlementation particulière en termes d'anonymisation des prises en charge ;
- d'autres situations de création d'identités fictives (traits imaginaires attribués à un patient incapable de décliner son identité, tests informatiques, formation…).

Remarque : la notion d'identité fictive est à différencier des situations « confidentielles » ou « protégées » où l'usager est inscrit sous sa véritable identité mais ne souhaite pas qu'on divulgue sa présence.

Pour les identités numériques comportant un attribut *Identité douteuse* ou *Identité fictive*, il doit être informatiquement rendu impossible :

- d'attribuer un statut autre que celui d'*Identité provisoire* ;
- de faire appel au téléservice INSi. [Exi SI 09]

Matrice récapitulative des associations possibles entre statuts et attributs :

---

[12] En dehors du cas d'usage spécifique d'un sous-traitant renvoyant les résultats d'un acte avec l'INS adressé par le prescripteur (cf. annexe 2)

[13] Des outils spécifiques pour la gestion de ces identités approchantes peuvent être proposés par les éditeurs informatiques

		Statuts			
		Id provisoire	Id récupérée	Id validée	Id qualifiée
Attributs	Id homonyme	+	+	+	+
	Id douteuse	+			
	Id fictive	+			

3.3.3 Bonnes pratiques de validation de l'identité numérique

3.3.3.1 Règles générales

Habituellement, la procédure validation et/ou de qualification de l'identité se fait à l'occasion d'une venue de l'usager, en lui demandant de présenter un document attestant son identité ou en utilisant un dispositif d'identification à haut niveau de confiance (cf. 3.3.3.2).

Afin d'utiliser une identité numérique de confiance, il est indispensable de s'assurer, *a minima* lors du premier contact physique de l'usager dans une structure, que les justificatifs d'identité présentés correspondent bien à la personne prise en charge. [Exi PP 08]

Lors de venues ultérieures, ce contrôle de cohérence systématique entre l'identité réelle et celle enregistrée peut ne pas se justifier si l'usager est connu de l'acteur de santé. En structure d'exercice collectif, il convient d'évaluer le niveau de risque en fonction de la population accueillie, des actes réalisés et du turnover des professionnels.

Par exemple, une demande d'attestation d'identité à chaque venue peut être rendue systématique pour les structures ou services qui pratiquent des activités à risque ou réalisent des accueils en urgence…

La structure peut décider de réaliser le contrôle de cohérence entre l'identité numérique et l'identité présente sur la pièce d'identité de façon différée (en *backoffice*) par des professionnels dédiés, sous couvert d'une procédure *ad hoc.* Dans ce cas, la pièce d'identité présentée doit avoir été sauvegardée par photocopie ou numérisation[14]. Cette validation différée est une bonne pratique pour sécuriser cette étape lorsque le flux des usagers à accueillir est important et/ou que la multiplication des tâches peut faire baisser le niveau de vigilance des professionnels assurant l'accueil dans le service concerné.

À l'inverse, la pratique de validation « automatique », sans s'appuyer sur un document d'identité de haut niveau de confiance (ou équivalent numérique), est une pratique dangereuse pour toutes les parties prenantes.

Il est formellement interdit de procéder à la validation d'une identité numérique sans pouvoir contrôler sa cohérence à la lumière d'un titre d'identité à haut niveau de confiance, ou de son équivalent numérique, dont le type est dûment enregistré dans le système d'information. [Exi PP 09]

[14] Sous réserve du respect des règles de conservation des données en vigueur

3.3.3.2 Quels sont les dispositifs permettant de valider ou de qualifier une identité ?

Seuls les dispositifs officiels à haut niveau de confiance sont acceptés pour modifier le statut *Identité Provisoire* en *Identité validée* ou celui d'*Identité récupérée* en *Identité qualifiée*.

Pour les usagers français, il s'agit de la carte nationale d'identité et du passeport[15]. Pour les mineurs qui n'en disposent pas, il est accepté le livret de famille ou un extrait d'acte de naissance, à condition de pouvoir vérifier l'identité du parent ou tuteur légal qui présente ces documents. Pour les usagers étrangers, il s'agit du passeport, du titre permanent de séjour, ou, pour les ressortissants de l'Union européenne (UE), de la carte d'identité nationale.

Tous les autres documents ont une valeur probante plus faible et ne permettent pas de valider une identité numérique.

Des dispositifs d'identification électronique peuvent aussi être employés. Pour autoriser la validation d'une identité numérique en santé, il faut que celui qui est utilisé apporte un niveau de garantie « substantiel » ou « élevé » au sens du règlement eIDAS[16].

Remarque : la présentation d'un document d'identité à haut niveau de confiance dont la date de validité est dépassée n'empêche pas d'attribuer le statut *Identité validée*. En cas de divergences entre 2 titres d'identités à haut niveau de confiance, il faut privilégier le passeport s'il fait partie des pièces présentées. Dans les autres cas, il faut prendre en compte les données du document le plus récent.

Les cas particuliers doivent faire l'objet d'une décision au cas par cas et signalés au niveau régional voire national.

Le type de dispositif d'identité ayant servi au recueil de l'identité doit être enregistré[17]. Seul un document à haut niveau de confiance, ou son équivalent numérique, doit autoriser l'attribution des statuts *Identité validée* ou *Identité qualifiée*. [Exi SI 10]

3.4 Utilisation pratique des traits d'identités

3.4.1 Quelles sont les règles applicables à l'affichage et l'édition des traits d'identité ?

Sauf réglementation applicable aux situations d'identités sensibles, les traits d'identité enregistrés dans le dossier de l'usager doivent pouvoir être accessibles à l'ensemble des professionnels qui partagent les données de santé, sans qu'il puisse y avoir de doute sur la nature de chaque trait affiché.

L'affichage du matricule INS n'est indispensable que pour les acteurs de santé ayant besoin de cette information. Les professionnels concernés sont à définir par la structure. Il peut être remplacé par un code et/ou une couleur indiquant le statut de l'identité.

---

[15] Loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité

[16] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

[17] La CNIL reconnait le caractère légitime de l'enregistrement d'une pièce d'identité dans le cadre de la vérification d'identité. Elle autorise la conservation d'une copie papier dans les mêmes conditions que le dossier médical pour une durée de cinq ans à compter de la dernière venue du patient dans l'établissement, la conservation des pièces d'identité numériques sous forme chiffrée, et l'accès à cette copie aux professionnels spécifiquement habilités en charge du traitement des anomalies liées à l'identité sous condition de traçabilité et d'historisation des consultations. Le stockage du numéro de la pièce est interdit.

Il est important que la nature de chaque trait d'identité affiché sur les documents et les interfaces homme machine soit facilement reconnue, sans risque d'équivoque, par tous les acteurs de santé concernés. [Exi SI 11]

Il appartient à la structure de santé de définir les modalités d'affichage et d'édition des traits dans les différents cas d'usage (interface homme machine, étiquettes, demande d'examen ou de prescription d'un acte, compte-rendu d'examen ou de séjour…), dans le respect de la réglementation en vigueur.

Il doit être affiché *a minima* les traits stricts suivants : nom de naissance, premier prénom de naissance, date de naissance, sexe et, sur les documents comportant des données d'information de santé, le matricule INS suivi de sa nature (NIR ou NIA) lorsque cette information est disponible et que son partage est autorisé. [Exi PP 10]

Remarque : lorsqu'ils sont renseignés, il est recommandé de faire apparaître également les champs *nom utilisé* et *prénom utilisé* sur les différents supports utilisés.

Des exemples pratiques sont donnés en Annexe VIII.

Dans le cas dérogatoire de l'identification des prélèvements biologiques, si un système permettant de relier de façon fiable un identifiant à l'identité de l'usager prélevé est utilisé par le préleveur, les traits d'identités peuvent ne pas figurer sur l'étiquette présente sur le tube.

Plus généralement, en complément d'un affichage « en clair », les identités INS sont présentées sous forme d'un datamatrix.

3.4.2 Comment utiliser les traits INS ?

Les modalités d'acceptation de l'identité renvoyée par le téléservice INSi sont développées en Annexe VI.

Après attribution du statut *Identité qualifiée* ou *Identité récupérée*, les traits INS doivent remplacer, si cela n'est pas déjà le cas, les traits stricts locaux dans les champs correspondants. [Exi SI 12]

Ces modifications doivent être transmises dans les logiciels tiers utilisés par la structure pour la prise en charge de l'usager.

Dès lors que son identité est passée au statut *Identité qualifiée*, le matricule INS et les traits INS doivent être utilisés pour l'identification de l'usager, notamment lors des échanges de données de santé le concernant. [Exi PP 11]

Remarque : d'autres identifiants nécessaires à la coordination des échanges peuvent continuer à être transmis.

Un certain nombre de situations d'anomalies peuvent survenir dans la gestion de l'identité, soit du fait d'écarts qui se révèlent *a posteriori*, soit en rapport avec une mauvaise attribution de l'identité INS. Ces situations font l'objet d'un chapitre dédié dans les volets du RNIV adaptés aux types de structures.

4 Gestion des risques liés à l'identification des usagers

La version socle du RNIV ne fait qu'évoquer les principes généraux d'organisation de la lutte contre les événements indésirables associés aux erreurs d'identification. Des éléments plus opérationnels en termes de politique, de gouvernance et de conduite de la gestion des risques à mettre en œuvre par les structures de santé sont développés dans les volets du RNIV adaptés aux types de structures.

4.1 Généralités

La gestion des risques (GDR) est indissociable de la démarche d'amélioration continue de la qualité. Elle est classiquement distinguée en 2 approches complémentaires selon le moment où l'action est menée :

- la GDR *a priori,* focalisée sur la prévention des risques évitables ;
- la GDR *a posteriori,* destinée à détecter et analyser les dysfonctionnements pour éviter qu'ils ne se reproduisent.

Les techniques de GDR appliqués aux erreurs d'identification primaire ou secondaires ne diffèrent pas de celles qui sont appliquées en routine dans les structures pour les autres types de risques, selon les recommandations de la Haute autorité de santé (HAS)[18].

Elles reposent notamment sur :

- une *cartographie de risques* a priori qui vise à recenser les situations connues d'erreurs d'identification, de les catégoriser en termes de niveau de criticité[19] (élevé, moyen ou faible) et à identifier les mesures à mettre en œuvre pour les prévenir ;
- la mise en œuvre de *mesures barrières* décrites dans une *documentation qualité* spécifique à l'identitovigilance ;
- un *système de signalement des événements indésirables* – potentiels ou avérés – qui permet d'identifier de nouvelles situations de dysfonctionnements en termes d'identification primaire et secondaire [20];
- des *retours d'expériences* (REX) qui visent à analyser les facteurs institutionnels, organisationnels et humains ayant conduit à l'erreur et à mettre en place des actions correctives et/ou préventives adaptées ;
- la formalisation de *procédures* précisant la conduite à tenir dans les activités à plus haut niveau de risque d'erreurs ;
- la formation des professionnels.

4.2 GDR liée à l'identification primaire

4.2.1 Sécurité des identités numériques

Les règles relatives à la sécurité des identités numériques dans les SIS ne sont pas spécifiques à l'identitovigilance mais elles ont une forte influence sur la sécurité des prises en charge des usagers.

Le présent document se contente d'en rappeler quelques principes tels que la nécessité :

---

[18] https://www.has-sante.fr/jcms/c_1661118/fr/gerer-les-risques

[19] Produit de la gravité et de la fréquence

[20] https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil

- de disposer d'un *référentiel unique d'identités* par structure (ou groupe de structures) afin de garantir la cohérence des données d'identité pour l'ensemble des logiciels métiers partageant des informations nominatives des usagers pris en charge ;
- d'établir une *cartographie de flux applicatifs* décrivant le type d'interface mis en œuvre entre les outils participant à l'identification des usagers ;
- de formaliser la *politique d'habilitation* et les droits individuels nominatifs (accès, modifications) attribués aux professionnels ;
- d'interdire l'utilisation de login génériques…

Les structures doivent disposer d'un référentiel unique d'identités assurant la cohérence des données pour l'ensemble des logiciels gérant des informations nominatives des usagers. [Exi SI 13]

Les structures doivent disposer d'une cartographie applicative détaillant en particulier les flux relatifs aux identités. Les outils non interfacés nécessitant une intervention humaine pour mettre à jour les identités doivent être identifiés. [Exi PP 12]

Une charte informatique formalisant les règles d'accès et d'usage du système d'information, et en particulier pour les applications gérant des données de santé à caractère personnel, doit être élaborée au sein de chaque structure à exercice collectif. [Exi PP 13]

Il est indispensable que les accès et les modifications apportées aux identités soient tracés (date, heure, type de modification et professionnel ayant réalisé l'action). Les récupérations successives de l'INS doivent également être enregistrées. [Exi SI 14]

La charte informatique est diffusée aux professionnels présents ainsi qu'aux nouveaux arrivants, sans oublier les prestataires et intervenants extérieurs.

4.2.2 Gestion des anomalies dans les bases d'identités

La structure doit régulièrement évaluer la qualité du référentiel d'identité (cf. 4.2.1) de chacun des domaines d'identification (cf. Annexe I) afin de pouvoir détecter et traiter les anomalies les plus courantes, chaque fois que c'est possible :
- doublons (plusieurs identités numériques correspondant à un même individu) ;
- collisions (même identité numérique attribuée à 2 individus différents) ;
- dates de naissances incohérentes ;
- sexe incohérent avec le prénom…

Il est recommandé que le système d'information dispose de fonctionnalités dédiées à la recherche des anomalies portant sur l'enregistrement des traits d'identité. [Reco SI 02]

4.2.3 Sécurité d'emploi de l'identité INS

4.2.3.1 Généralités

Les erreurs associées à l'emploi de l'identité INS ont des conséquences potentiellement plus importantes car elles peuvent être propagées à l'extérieur de la structure (cf. 1.1). Il est donc nécessaire de mettre en place une vigilance particulière dans ce domaine et de prévoir les consignes à donner face aux différents types d'événements indésirables pouvant se produire.

Il est important de formaliser des procédures qui précisent la conduite à tenir :
- pour la retranscription d'une identité INS reçue sur format papier (cf. 4.2.3.2) ;
- quand il est constaté une divergence avérée entre l'identité numérique locale et les traits INS à l'occasion d'un appel INSi (cf. Annexe VI), que ce soit lors d'une recherche initiale ou d'une opération de vérification (cf. 4.2.3.3 et 4.2.3.4) ;
- lorsque la qualification de l'identité numérique n'est pas possible à court terme faute de présentation de documents d'identité à haut niveau de preuve ;
- en cas d'erreur d'attribution d'un matricule INS à un usager (modalités d'information de l'ensemble des acteurs avec lequel la structure a partagé des données en utilisant ce mauvais identifiant).

Les acteurs de santé impactés par la diffusion d'une erreur en lien avec l'identité INS doivent être alertés sans délai, selon une procédure spécifique formalisée par la structure. [Exi PP 14]

4.2.3.2 Retranscription de l'identité INS reçue sous format papier

Pour éviter les erreurs de retranscription manuelle, il est nécessaire de faire appel, en l'absence de l'usager, au téléservice INSi de récupération par recherche des traits (cf. 3.2.1.3). Si l'identité a été retranscrite manuellement avec le matricule INS, l'appel au téléservice INSi de vérification est obligatoire (cf. 3.1.2.3 et Exi PP 01).

4.2.3.3 Anomalie relevée lors de la vérification de l'identité à la réception de données de santé

Une opération de vérification est à réaliser par le destinataire lors de la réception de données de santé associées à une identité INS pour un usager ne disposant pas encore, à son niveau, d'une identité numérique au statut *Identité qualifiée*. Si la vérification n'est pas concluante, le matricule INS ne doit pas être enregistré. Après recherche d'antériorité dans la base locale (cf. 3.1.1.1), les données de santé pourront, selon la situation :
- être associées à une nouvelle identité numérique locale créée avec les traits de l'identité reçue, au statut *Identité provisoire* ;
- être associées à une identité non qualifiée existante partageant les mêmes traits stricts, sous réserve que le professionnel soit certain de ne pas créer de collision ;
- ne pas être intégrées dans le système d'information, faute de pouvoir les attribuer en toute sécurité à un usager défini, mais servir à alimenter une liste d'anomalies à traiter.

Dans tous les cas, il est nécessaire d'adresser une alerte à l'expéditeur des données pour lui signaler l'existence de l'anomalie (cf. Exi PP 14) et de rechercher la cause de l'incohérence signalée par le téléservice (cf. Annexe VI).

4.2.3.4 Anomalie relevée lors de la vérification systématique de la base d'identités

Le référentiel INS[21] précise qu'une opération de vérification des identités qualifiées doit être programmée tous les 3 à 5 ans. En cas de retour négatif du téléservice INSi concernant une identité numérique, le risque majeur est d'utiliser et de transmettre une identité INS invalide. Une procédure doit préciser comment gérer cette situation. En attendant de comprendre l'origine de l'échec de l'opération, il faut notamment :

[21] https://esante.gouv.fr/sites/default/files/media_entity/documents/ASIP_R%C3%A9f%C3%A9rentiel_Identifiant_National_de_Sant%C3%A9_v1.pdf

- changer le statut de l'identité numérique en ***Identité validée*** – s'il est possible de contrôler de nouveau la cohérence de l'identité à partir d'un document à haut niveau de confiance numérisé – ou en ***Identité provisoire*** dans le cas contraire ;
- supprimer (ou invalider) le matricule INS.

4.3 GDR liée à l'identification secondaire

Les bonnes pratiques d'identification primaire ne permettent pas, à elles seules, de sécuriser la prise en charge des usagers. Il faut encore que les professionnels s'assurent que l'usager bénéficiaire de l'acte est bien celui pour lequel le soin a été prescrit. Parmi les préconisations qui sont faites pour faciliter cette identification secondaire, on peut citer :

- la participation active de l'usager, chaque fois que possible, à la sécurité de ses soins et donc à la vérification de son identité avant les soins, et notamment avant les actes à risques (« patient acteur de sa sécurité ») ;
- l'utilisation, lorsqu'ils existent, du nom utilisé et du prénom utilisé pour les échanges directs avec l'usager ;
- la mise en œuvre de dispositifs d'identification physique tels que la pose d'un bracelet, l'utilisation d'une photographie dans le dossier de l'usager[22] ;
- la réalisation régulière de contrôles de cohérence entre l'identité de l'usager (déclinée ou vérifiée sur le dispositif d'identification physique) et celle relevée sur les documents (prescription, plan de soins, pilulier, étiquette, comptes rendus, résultats d'examens…) ;
- la vérification de la cohérence – en termes d'affichage, de présence et de nommage des champs relatifs à l'identité – entre les différents logiciels échangeant des données de santé de l'usager au sein de la structure.

4.4 Documentation qualité

Les structures de santé d'exercice collectif doivent formaliser la politique institutionnelle d'identification de l'usager au sein d'une charte d'identitovigilance. [Exi PP 15]

La charte d'identitovigilance, qui peut être commune à plusieurs structures associées, a pour objet de rappeler les principes à respecter pour :

- recueillir l'identité des usagers ;
- prévenir les risques liés à une mauvaise identification ;
- harmoniser les pratiques et favoriser l'acculturation de la sécurité des professionnels ;
- impliquer les usagers dans cette exigence de sécurité.

Elle se décline à travers des procédures opérationnelles mises en œuvre au sein de la structure – ou du groupe de structures – en fonction des risques identifiés et de leur criticité (cf. 4.1).

4.5 Indicateurs qualité

Les indicateurs qualité ont pour but d'évaluer la performance du système. Il est important d'en disposer à la fois sur les pratiques d'identification primaire et secondaire. Ils sont définis au sein de la structure mais peuvent aussi faire l'objet d'une généralisation territoriale, régionale voire nationale. Ils sont précisés dans les volets déclinant la politique et la gestion des risques dans les différents types de structures.

[22] Sous réserve du respect du droit à l'image et de la réglementation applicable

4.6 Formation et sensibilisation à l'identitovigilance

Le respect des règles d'identification repose sur leur compréhension et leur appropriation par toutes les parties prenantes : professionnels comme usagers. Ce domaine nécessite donc une attention particulière en termes :

- de formation et de sensibilisation de l'ensemble des professionnels de la structure ;
- d'évaluations régulières des connaissances et des pratiques ;
- d'information et de sensibilisation des correspondants externes (ambulanciers, professionnels et structures adressant des usagers, plateaux techniques…) ;
- d'information et de sensibilisation des usagers.

ANNEXE I – Domaines d'identification et de rapprochement

Personne physique  et identité numérique 

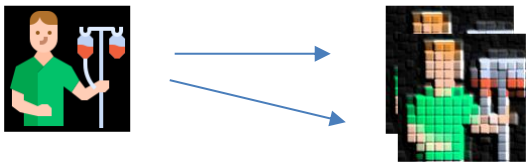
Toute personne physique enregistrée dans un système d'information y est reconnue via son identité numérique. Celle-ci comporte *a minima* :

- un domaine d'identification (DI) qui identifie la base de données d'identités utilisée ;
- l'identifiant local (I) utilisé dans cette base pour identifier l'usager ;
- un jeu de traits d'identité (T) caractérisant celui-ci (nom, adresse, etc.) ;
- un statut (S) qui précise le niveau de confiance de cette identification.

Domaine d'identification (DI)

Un domaine d'identification rassemble l'ensemble des applications informatiques où l'usager est reconnu par une même identité numérique, à travers une base d'identités commune.

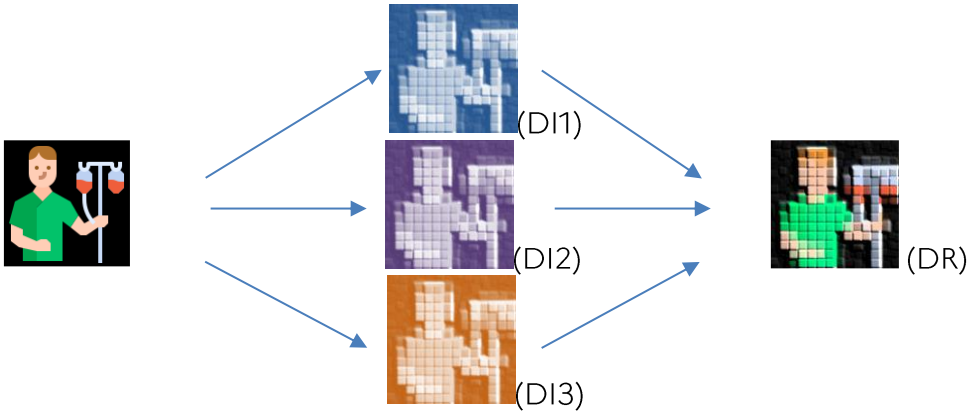
Dans un DI, un doublon correspond à l'identification d'une même personne physique sous plus d'une identité numérique (I1, I2…).



Dans un DI, une collision correspond à l'identification de 2 personnes physiques différentes avec la même identité numérique.

Domaine de rapprochement (DR)

Un domaine de rapprochement attribue une identité numérique commune (dite identité de fédération) à plusieurs domaines d'identification qui peuvent ainsi échanger en toute sécurité des données. Il sert de référentiel unique d'identités.



ANNEXE II - Terminologie et définitions

Cette annexe définit un certain nombre de termes employés par les professionnels de l'identitovigilance.

Acteur de santé

Ce terme est utilisé de façon générique, dans ce document, pour identifier les professionnels intervenant dans la prise en charge sanitaire ou médico-sociale ou sociale d'un usager.

Alias = pseudonyme

Ayant droit

Usager non assuré à titre personnel mais pouvant bénéficier des droits aux prestations sociales en raison d'un lien, qui est souvent d'ordre familial, avec l'assuré ouvrant droit.

Code officiel géographique (COG)

C'est le mode de codage utilisé pour enregistrer le lieu de naissance pour les personnes nées en France, à partir des tables fournies par l'INSEE. Le COG de la commune étant susceptible d'évoluer dans le temps, c'est celui récupéré avec l'identité INS qui fait fois en cas de divergence liée à l'historique du codage de la commune.

Collision

C'est une anomalie correspondant à l'attribution d'un même identifiant à 2 personnes physiques différentes, ou plus, notamment dans les cas suivants : sélection erronée d'un dossier informatique, usurpation d'identité d'un tiers déjà enregistré, erreur d'opération de fusion entre dossiers n'appartenant pas au même usager… Il devient très difficile dans ce cas de faire la part, *a posteriori*, des informations médicales qui relèvent de chaque usager. Le risque est de prendre des décisions médicales et soignantes au regard des données de santé d'une autre personne.

Date de naissance

Elle fait partie des traits stricts de l'identité et doit être saisie sous le format JJ/MM/AAAA, ce qui nécessite la transformation dans ce format des dates libellées dans un calendrier luni-solaire pour les usagers nés à l'étranger.

Domaine d'identification

Il regroupe au sein d'une organisation de santé toutes les applications qui utilisent le même identifiant pour désigner un patient.

Exemples :

- un cabinet médical disposant d'un mode unique d'identification de ses patients est considéré comme un domaine d'identification ;
- un établissement de santé dont tous les logiciels utilisent le même identifiant est un domaine d'identification.

Domaine de rapprochement

Il rassemble au moins deux domaines d'identification qui échangent ou partagent des informations entre eux. On distingue les domaines de rapprochements intra établissement et extra établissement.

Exemples :

- un établissement de santé disposant d'un Identifiant Permanent du Patient (IPP) et dont une partie des logiciels utilise un identifiant et une autre partie des logiciels un autre identifiant est un domaine de rapprochement. En effet, dans cet exemple, il existe deux groupes de logiciels et chaque groupe utilise un identifiant qui lui est propre. Chaque groupe constitue donc un domaine d'identification différent. L'établissement dispose également d'un IPP qui lui permet d'échanger des informations entre les deux domaines d'identification. Ce domaine de rapprochement est un domaine de rapprochement intra établissement ;
- si des établissements de santé alimentent un serveur régional d'identité et de rapprochement, alors ce serveur constitue un domaine de rapprochement.

Données de santé

Données à caractère personnel relatives à la santé physique ou mentale qui révèlent des informations sur l'état de santé de cette personne. Elles comprennent les informations :

- collectées en vue de bénéficier de prestations de santé (identifiants, traits d'identité) ;
- obtenues lors de la prise en charge (antécédents, résultats d'examens, informations échangées entre professionnels…) ;
- à partir desquelles il est possible de déduire une information sur l'état de santé de la personne (prestation de soins, service hospitalier…).

Doublon

On parle de doublons d'identités lorsqu'une même personne est enregistrée sous 2 identifiants différents (ou plus) dans un même domaine d'identification. On dispose alors pour l'usager de plusieurs dossiers médicaux et administratifs différents qui ne communiquent pas entre eux. Le fait de ne pas disposer de l'ensemble des informations médicales concernant l'usager engendre un risque lié à la méconnaissance, par le professionnel, de données utiles à la prise de décision.

D*oublon de flux* : doublon dépisté dans la file active à l'occasion de la venue d'un usager.

D*oublons de stock* : ensemble des doublons présents dans le référentiel d'identités. Les doublons de stock peuvent être identifiés lors de l'analyse de la qualité des bases patients.

État civil

En droit français, l'état civil est constitué des éléments qui permettent l'identification d'une personne, tels que le nom, le ou les prénoms, le sexe, la date et le lieu de naissance, la filiation, la nationalité, le domicile, la situation matrimoniale, la date et le lieu de décès. Toute personne vivant habituellement en France, même si elle est née à l'étranger et possède une nationalité étrangère, doit être pourvue d'un état civil.

Fusion

Elle correspond au transfert, sur un identifiant unique, de toutes les informations concernant le même usager dispersées sur plusieurs identifiants (doublons) d'un même domaine d'identification.

Homonyme

L'homonymie est définie comme la correspondance exacte entre plusieurs traits stricts partagés par plusieurs personnes différentes. Ces usagers homonymes doivent donc être différenciés à l'aide d'autres traits.

La notion d'homonymie est à rapprocher de la notion d'identités proches ou approchantes où les traits sont différents mais peuvent potentiellement être confondus (exemple : Dupond et Dupont).

Identifiant (technique)

Séquence de caractères alphanumériques utilisée par un ou plusieurs systèmes d'information pour représenter une personne physique. Par exemple : identifiant permanent du patient (IPP), matricule INS…

Identité nationale de santé (INS)

C'est une identité numérique unique, univoque, pérenne, permettant de référencer, de conserver et de transmettre les informations de santé d'un usager. Son utilisation est obligatoire à compter du 01/01/2021 par l'ensemble des professionnels de santé. Elle correspond aujourd'hui à l'*identité INS* (cf. ce terme).

Remarque : un identifiant calculé (INS-C), attribué au travers d'un algorithme à partir d'informations lues à partir de la carte Vitale de l'assuré, a d'abord été utilisé mais les résultats se sont révélés être à l'origine de doublons ou de collisions.

Identification primaire

C'est l'ensemble des opérations destinées à attribuer de manière univoque à une personne physique une identité numérique qui lui est propre. L'identification primaire comprend les étapes de recherche d'un patient dans la base, de création ou de modification d'une identité, de validation de cette identité, de récupération de l'identité INS via l'appel au téléservice INSi.

Identification secondaire

Elle correspond à la vérification, par tout professionnel de santé, de l'identité de l'usager physique tout au long de sa prise en charge avant la réalisation d'un acte le concernant (prélèvement, soins, transport, acte technique…). Elle comprend également l'identification des prélèvements ou des documents de l'usager et la sélection du bon dossier dans une application utilisée au sein d'un service de soins (prescription, dossier de soins, résultats d'examens…).

Identité

Ensemble de données, ou traits d'identité, qui constituent la représentation d'une personne physique.

Identité douteuse

Attribut d'une identité numérique utilisé pour signaler que la procédure d'identification n'est pas sûre, soit du fait d'un doute sur le document d'identification présenté (suspicion de fraude), soit parce l'identité est relevée sur les dires d'un patient confus ou d'un tiers qui le connait mal. C'est un attribut qui ne peut être associé qu'au statut d'identité provisoire.

Identité fictive

Attribut d'une identité numérique utilisé pour signaler que les traits d'identité n'ont pas de rapport avec l'identité réelle de l'usager. Il découle de la mise en œuvre d'une procédure d'identification applicable aux situations d'identités sensibles (anonymisation de la prise en charge). Cet attribut peut également servir dans le cadre de tests informatiques ou de formations. C'est un attribut qui ne peut être associé qu'au statut d'identité provisoire.

Identité frauduleuse

Le terme d'identité frauduleuse s'applique aux situations où un usager utilise l'identité d'un autre afin de bénéficier de droits sociaux auxquels lui-même n'a pas droit. Cette situation peut engendrer des risques très graves pour la santé du fraudeur comme du titulaire des droits lors d'un prochain séjour dans l'établissement de soins par le mélange des informations (collision)

qu'elle entraîne dans un même dossier patient. Elle doit faire l'objet, quand elle est suspectée, de l'utilisation de l'attribut Identité douteuse.

Identité homonyme

Attribut utilisé pour signaler un fort taux de ressemblance entre des identités numériques et alerter les professionnels lors de la prise en charge de ces usagers homonymes ou à identités approchantes.

Identité INS

Ensemble des informations numériques renvoyés par le téléservice INSi, constituées :

- du matricule INS : numéro d'identification au répertoire des personnes physiques (NIR ou NIA) ;
- des traits INS (Nom de naissance, liste des prénoms de l'état civil, date de naissance, sexe, code commune du lieu de naissance ou code pays pour les personnes nées à l'étranger) ;
- de l'OID (*object identifier*) qui identifie l'origine et le type de l'information (INSEE, NIR/NIA…).

Identité numérique

L'identité numérique correspond à la représentation d'un individu physique dans un système d'information (cf. Annexe I). Un même usager peut avoir plusieurs identités numériques : dans le (ou les) domaines d'identification ou de rapprochement utilisés par la structure, dans son dossier médical partagé (DMP), dans la base de données de facturation de l'assurance maladie… En revanche, lorsque l'usager a plusieurs identités numériques dans un même domaine d'identification, il s'agit de doublons.

Identité provisoire

Statut d'une identité numérique locale qui n'a pas été récupérée sur le téléservice INSi et qui n'a pas encore fait l'objet d'un contrôle de cohérence avec les traits portés par un dispositif d'identité à haut niveau de confiance. Ce statut peut, si besoin, être associé à un attribut *Identité douteuse* ou *Identité fictive*.

Identité qualifiée

Statut d'une identité numérique locale qui a été récupérée sur le téléservice INSi, et comparée avec succès aux traits de la personne physique portés par un dispositif d'identité à haut niveau de confiance.

Identité récupérée

Statut d'une identité numérique locale qui a été récupérée sur le téléservice INSi après avoir été comparée avec succès aux traits de la personne physique mais qui n'a pas encore pu être contrôlée à partir d'un document d'identité à haut niveau de confiance.

Identité sensible

Le terme d'identité sensible s'utilise de façon générique pour regrouper tous les cas où il existe un droit renforcé par la réglementation vis-à-vis de la confidentialité, notamment en termes d'anonymat des soins.

Identité validée

Statut d'une identité numérique qui n'a pas été récupérée sur le téléservice INSi mais qui a fait l'objet d'un contrôle de cohérence avec le jeu de traits portés par un dispositif d'identité à haut niveau de confiance, ce qui garantit l'absence d'erreur dans l'enregistrement des traits d'identité d'un usager.

Identité test

Identité fictive créée pour évaluer le fonctionnement d'un système d'information dans le cadre d'une création, d'une modification ou d'une mise à jour. Dans une base d'identité réelle, elle doit faire l'objet de l'utilisation de l'attribut Identité douteuse.

Identitovigilance

Politique, organisation et moyens mis en œuvre pour fiabiliser l'identification d'un usager à toutes les étapes de sa prise en charge.

INSi

Service en ligne de la CNAM permettant de rechercher et de télécharger l'identité INS.

Jeux de traits

Ensemble des caractéristiques (ou traits) d'un usager qui permettent de le décrire de manière univoque.

Lieu de naissance

Identification du lieu de naissance qui comporte plusieurs paramètres renseignés dans les traits stricts et complémentaires : nom de la commune, code postal et code officiel géographique de l'INSEE pour les personnes nées en France ; pays et code INSEE du pays pour les personnes nées à l'étranger.

Matricule INS

Identifiant de l'identité INS, représenté par le NIR ou le NIA personnel de l'usager.

Moyen d'identification électronique

Élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne.

NIA

C'est le *numéro d'immatriculation d'attente* (NIA) attribué par la CNAV aux personnes nées à l'étranger à partir des données d'état civil (art. R.114-26 du code de la sécurité sociale). Le NIA devient NIR lorsque l'identité de la personne est confirmée et qu'aucun doublon n'est possible avec un autre NIR. En l'absence de NIR, le NIA constitue le matricule INS des personnes prises en charge dans les champs sanitaire et médico-social (articles L.1111-8-1, R.1111-8-1 et suivants du code de la santé publique).

NIR

Le *numéro d'inscription au répertoire des personnes physiques* (NIRPP ou NIR) sert à identifier une personne dans le répertoire national d'identification des personnes physiques géré par l'INSEE (RNIPP).

Le NIR personnel constitue le matricule INS des personnes prises en charge dans les champs sanitaire et médico-social (articles L.1111-8-1, R.1111-8-1 et suivants du code de la santé publique).

Le NIR est attribué :

- soit par l'INSEE lors de l'inscription au RNIPP ; l'inscription a lieu, en général, au plus tard huit jours après la naissance, à partir de l'état civil transmis par les mairies (sexe, année et mois de naissance, département et commune de naissance, numéro d'ordre du registre d'état civil) ;
- soit par la CNAV lors de l'inscription sur le système national de gestion des identités (SNGI) à la demande d'un organisme de sécurité sociale, à l'occasion d'une démarche effectuée par la personne elle-même ou par son employeur.

Les deux systèmes sont synchronisés quotidiennement.

Nom de famille

Le terme *nom de famille* a officiellement succédé à celui de *nom patronymique* ou *nom de naissance* ou *nom de jeune fille*. Il est transmis selon des règles propres à la filiation. Il est toujours intégré dans l'extrait d'acte de naissance.

Le changement de nom de famille est prévu par les articles 60 à 62-4 du code civil. Il peut être lié à la procédure de francisation du nom et/ou des prénoms pour les personnes qui acquièrent ou recouvrent la nationalité française.

Remarque : Pour une meilleure compréhension, il a été choisi de continuer d'utiliser le terme *nom de naissance* dans le RNIV car les usagers ont tendance à confondre *nom de famille* et *nom d'usage*.

Nom de jeune fille (désuet) = nom de famille = nom de naissance

Nom marital (désuet) : voir nom d'usage

Nom de naissance = nom de famille

Nom patronymique (désuet) = nom de famille = nom de naissance

Nom d'usage

Le *nom d'usage* est un nom hérité d'un acte d'état civil (mariage, naissance…). Il est normalement précisé sur un document officiel d'identité après le titre « Nom d'usage ».

Il peut évoluer au gré des actes d'état civil (divorce, remariage). Faute de mise à jour des pièces d'identité, il est parfois en discordance avec le nom réellement porté par l'usager, ce qui n'en fait pas un trait d'identité fiable, et ce d'autant que l'usager peut décider de ne pas le porter dans tout ou partie de ses activités.

Remarque : il est recommandé de préférer le terme *nom d'usage* à celui, désuet, de *nom marital*.

Nom usuel = nom d'usage

Nom utilisé

A la place du *nom d'usage*, qui a une définition légale, le RNIV crée le terme de *nom utilisé* pour permettre l'enregistrement du nom réellement porté dans la vie courante, qu'il s'agisse du *nom de naissance* ou du n*om d'usage*, voire, sous certaines conditions, celui utilisé dans le *pseudonyme* ou le *surnom* de l'usager. Ce trait complémentaire a pour objet de faciliter le dialogue soignant-soigné.

Ouvrant droit

Personne affiliée à un régime d'assurance maladie obligatoire. Cette affiliation lui permet le cas échéant d'« ouvrir des droits » à d'autres personnes dites « ayant droits » (ses enfants mineurs par exemple).

Prénom(s) de naissance

L'attribution d'un prénom est obligatoire : il est indiqué sur l'acte de naissance. Il peut comporter plusieurs prénoms, ainsi que des prénoms composés.

Premier prénom de naissance

La distinction du *premier prénom* dans la liste des prénoms de naissance est nécessaire à la communication entre logiciels n'ayant pas encore été mis en conformité avec les exigences du RNIV. Il peut être composé (avec ou sans trait d'union entre les prénoms).

Prénom usuel

Tout prénom inscrit dans l'acte de naissance peut être choisi comme prénom usuel (art. 57 du code civil). Ce choix peut être précisé après la mention « Prénom usuel » en dessous la rubrique « Prénom(s) » du titre d'identité. Il arrive cependant que le prénom porté dans la vie courante, différent du premier prénom de naissance, n'ait jamais été officialisé.

Prénom d'usage = Prénom usuel

Prénom utilisé

À la place du *prénom usuel*, qui a une définition légale, le RNIV crée le terme de pr*énom utilisé* pour permettre l'enregistrement du prénom réellement porté dans la vie courante. Il peut s'agir d'un des *prénoms de naissance*, du *prénom d'usage* voire, sous certaines conditions, d'un autre prénom non officialisé – comme cela peut être habituel dans certaines régions – ou utilisé dans le *pseudonyme* ou le *surnom* de l'usager. Ce trait complémentaire a pour objet de faciliter le dialogue soignant-soigné.

Responsable de traitement

Selon le règlement général de protection des données (RGPD), le responsable de traitement est la personne morale (structure) ou physique (professionnel) qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

Pseudonyme

Identité d'emprunt ou « alias » librement choisie par une personne pour dissimuler son identité réelle dans l'exercice d'une activité particulière, notamment dans le milieu littéraire ou artistique. Il ne fait l'objet d'aucune réglementation particulière et ne peut être mentionné sur les actes d'état civil. Un pseudonyme peut toutefois figurer sur la carte d'identité si sa notoriété est confirmée par un usage constant et ininterrompu (exemple : « Johnny Halliday »). Il est précédé de la mention « Pseudonyme » ou de l'adjectif « Dit » sur une ligne spécifique[23].

Il peut être mentionné dans les champs *nom utilisé* et *prénom utilisé* à la triple condition que ce soit (1) sur demande expresse de l'usager, (2) un trait non susceptible de changer à chaque venue, (3) compatible avec la politique d'identitovigilance de la structure.

[23] À différencier du mot « dit » figurant sur la ligne du nom qui fait partie intégrante du nom de naissance de la personne

Rapprochement d'identités

Attribution d'une identité numérique (dite identité de fédération) commune à plusieurs identités numériques appartenant à des domaines d'identification différents (au niveau territorial, régional) mais qui font référence au même usager.

Référentiel unique d'identités

Ensemble de composants (techniques et organisationnels) du système d'information qui garantit la cohérence des données d'identité pour l'ensemble des logiciels métiers gérant des informations nominatives des usagers pris en charge.

Sexe

Le sexe est codé sous la forme M (masculin), F (féminin) ou I (indéterminé). L'identité INS ne peut comporter que des valeurs F ou M.

Structure de santé

Ce terme est utilisé de façon générique, dans ce document, pour identifier les établissements, cabinets libéraux, services et organismes intervenant dans la prise en charge sanitaire ou médico-sociale d'un usager.

Surnom ou sobriquet

C'est un trait d'identité qui peut être mentionnée sur l'acte de naissance si une confusion est à craindre entre plusieurs homonymes ; en pareil cas, il est précédé de l'adjectif « Dit » sur une ligne séparée du nom.

Il peut être mentionné dans les champs *nom utilisé* et *prénom utilisé* à la triple condition que ce soit (1) sur demande expresse de l'usager, (2) un trait non susceptible de changer à chaque venue, (3) compatible avec la politique d'identitovigilance de la structure.

Traits (d'identité)

Ce sont des éléments d'identification propres à un usager, d'importance variable : on distingue les traits stricts et les traits complémentaires (voir aussi : Jeu de traits).

Traits stricts

Ce sont des traits d'identité de référence qui permettent d'identifier officiellement une personne physique sans risque d'erreur : nom de naissance, prénom(s) de naissance, 1er prénom de naissance, date de naissance, sexe, pays de naissance (pour les patients nés à l'étranger) ou lieu de naissance (pour les patients nés en France, y compris les DOM, COM, POM), matricule INS.

Traits complémentaires

Ce sont des renseignements personnels, susceptibles d'évoluer dans le temps, qui apportent un supplément d'informations pour la bonne prise en charge de l'usager. Par exemple : nom et prénom utilisés, adresse…

Usager

Ce terme est utilisé de façon générique dans ce document pour identifier les personnes prises en charge par les structures de santé : patients, résidents.

Usurpation d'identité

Selon l'article 226-4-1 du Code pénal, il s'agit d'une infraction consistant à utiliser l'identité d'un tiers à des fins malveillantes. En santé, on a plutôt affaire à des situations d'utilisation frauduleuse

d'identité dans le but de bénéficier de la couverture sociale d'un autre usager, avec la complicité fréquente de celui-ci.

ANNEXE III – Exigences et recommandations

Exigences et recommandations communes relatives au système d'information

Exi SI 01	Le système d'information doit permettre, *a minima*, d'effectuer la recherche d'une identité numérique à partir : - de tout ou partie de l'identité INS récupérée après l'interrogation du téléservice INSi ; - de la saisie de la date de naissance, éventuellement complétée par les premiers caractères du nom ou du prénom.
Exi SI 02	L'utilisation du matricule INS pour la recherche d'antériorité doit être sécurisée pour éviter tout risque lié à une erreur de saisie. Si le matricule n'est pas récupéré électroniquement, la saisie des 15 caractères du NIR et leur validation par la clé de contrôle est obligatoire pour toute recherche à partir du matricule INS.
Exi SI 03	Lors de la recherche d'un usager dans la base d'identités, il est nécessaire que le système d'information interroge sans distinction, avec les données correspondantes mais sans tenir compte des tirets ou apostrophes, les champs *Nom de naissance* et *Nom utilisé*, ainsi que les champs *Prénom(s) de naissance*, *Premier prénom de naissance* et *Prénom utilisé*.
Exi SI 04	Les traits d'identification doivent faire l'objet de champs spécifiques dans le système d'information.
Exi SI 05	Le système d'information doit permettre la saisie des traits complémentaires *Nom utilisé* et *Prénom utilisé*.
Exi SI 06	Les informations récupérées du téléservice INSi font l'objet d'un stockage et d'une traçabilité au niveau du système d'information de santé.
Exi SI 07	Tout système d'information en santé doit permettre d'attribuer un des 4 statuts de confiance à chaque identité numérique stockée.
Exi SI 08	Le système d'information doit garantir que seul le statut *Identité qualifiée* permette le référencement des données de santé échangées avec le matricule INS, en conformité avec la réglementation applicable.
Exi SI 09	Pour les identités numériques comportant un attribut *Identité douteuse* ou *Identité fictive,* il doit être informatiquement rendu impossible : - d'attribuer un statut autre que celui d'*Identité provisoire* ; - de faire appel au téléservice INSi.
Exi SI 10	Le type de dispositif d'identité ayant servi au recueil de l'identité doit être enregistré. Seul un document à haut niveau de confiance, ou son équivalent numérique, doit autoriser l'attribution des statuts *Identité validée* ou *Identité qualifiée*.

Exi SI 11	Il est important que la nature de chaque trait d'identité affiché sur les documents et les interfaces homme machine soient facilement reconnues, sans risque d'équivoque, par tous les acteurs de santé concernés.
Exi SI 12	Après attribution du statut *Identité qualifiée* ou *Identité récupérée*, les traits INS doivent remplacer, si ce n'est pas déjà le cas, les traits stricts locaux dans les champs correspondants.
Exi SI 13	Les structures doivent disposer d'un référentiel unique d'identités assurant la cohérence des données pour l'ensemble des logiciels gérant des informations nominatives des usagers.
Exi SI 14	Il est indispensable que les accès et les modifications apportées aux identités soient tracés (date, heure, type de modification et professionnel ayant réalisé l'action). Les récupérations successives de l'INS doivent également être enregistrées.
Exi SI 15	Les systèmes d'information peuvent permettent de traduire dans le format JJ/MM/AAA les dates de naissance libellées dans un calendrier luni-solaire pour les usagers nés à l'étranger.
Reco SI 01	Il est recommandé que les systèmes d'information en santé autorisent l'emploi d'attributs supplémentaires pour permettre aux professionnels de caractériser les identités numériques nécessitant un traitement particulier.
Reco SI 02	Il est recommandé que le système d'information dispose de fonctionnalités dédiées à la recherche des anomalies portant sur l'enregistrement des traits d'identité.

Exigences communes relatives aux pratiques professionnelles

Exi PP 01	L'appel au téléservice INSi est obligatoire pour vérifier une identité INS reçue lorsque l'identité numérique n'existe pas ou qu'elle ne dispose pas d'un statut récupéré ou qualifié.
Exi PP 02	La création d'une identité numérique requiert la saisie d'une information dans au moins 5 traits stricts : nom de naissance, premier prénom de naissance, date de naissance, sexe et lieu de naissance.
Exi PP 03	Les champs relatifs à la liste des prénoms de naissance et au matricule INS sont renseignés dès qu'il est possible d'accéder à ces informations : présentation d'un titre d'identité et/ou appel au téléservice INSi, dans les cas d'usage où l'emploi du matricule INS est requis et autorisé.
Exi PP 04	Il est nécessaire de renseigner le maximum de traits complémentaires, selon les consignes que chaque structure définit en fonction de ses besoins.
Exi PP 05	Avant toute intégration de l'identité INS dans l'identité numérique locale, il est nécessaire de valider la cohérence entre les traits INS renvoyés par le téléservice INSi et les traits de la personne physique prise en charge.
Exi PP 06	L'interrogation du téléservice INSi par l'intermédiaire de la carte vitale est le mode d'interrogation à privilégier chaque fois que possible.
Exi PP 07	L'attribution d'un niveau de confiance à toute identité numérique est obligatoire.
Exi PP 08	Afin d'utiliser une identité numérique de confiance, il est indispensable de s'assurer, *a minima* lors du premier contact physique de l'usager dans une

	structure, que les justificatifs d'identité présentés correspondent bien à la personne prise en charge.
Exi PP 09	Il est formellement interdit de procéder à la validation d'une identité numérique sans pouvoir contrôler sa cohérence à la lumière d'un titre d'identité à haut niveau de confiance, ou son équivalent numérique, dont le type est dument enregistré dans le système d'information.
Exi PP 10	Il doit être affiché *a minima* les traits stricts suivants : nom de naissance, premier prénom de naissance, date de naissance, sexe et, sur les documents comportant des données d'information de santé, le matricule INS suivi de sa nature (NIR ou NIA) lorsque cette information est disponible et que son partage est autorisé.
Exi PP 11	Dès lors que son identité est passée au statut *Identité qualifiée*, le matricule INS et les traits INS doivent être utilisés pour l'identification de l'usager, notamment lors des échanges de données de santé le concernant.
Exi PP 12	Les structures doivent disposer d'une cartographie applicative détaillant en particulier les flux relatifs aux identités. Les outils non interfacés nécessitant une intervention humaine pour mettre à jour les identités doivent être identifiés.
Exi PP 13	Une charte informatique formalisant les règles d'accès et d'usage du système d'information, et en particulier pour les applications gérant des données de santé à caractère personnel, doit être élaborée au sein de chaque structure à exercice collectif.
Exi PP 14	Les acteurs de santé impactés par la diffusion d'une erreur en lien avec l'identité INS doivent être alertés sans délai, selon une procédure spécifique formalisée par la structure.
Exi PP 15	Les structures de santé d'exercice collectif doivent formaliser la politique institutionnelle d'identification de l'usager au sein d'une charte d'identitovigilance.
Exi PP 16	Comme pour les autres traits stricts, la date de naissance à enregistrer est celle établie d'après un document ou un dispositif officiel d'identité et non celle lue sur un document de l'Assurance maladie, qui peut être différente.
Exi PP 17	L'enregistrement du *nom utilisé* est obligatoire lorsqu'il est différent du *nom de naissance*.
Exi PP 18	L'enregistrement du *prénom utilisé* est obligatoire lorsqu'il est différent du *premier prénom de naissance*.
Reco PP 01	Pour obtenir des résultats pertinents, il est fortement recommandé de limiter le nombre de caractères saisis pour effectuer la recherche d'un enregistrement.
Reco PP 02	Il est important que toute difficulté rencontrée pour la récupération de l'identité INS ou la qualification de l'identité numérique, du fait d'une incohérence non mineure, soient signalée comme événement indésirable et rapportée au niveau régional et national[24].

Les exigences posées par le RNIV viennent en compléments de celle posées par le référentiel INS.

[24] Les modalités de signalement aux niveaux régional et national seront précisées ultérieurement

ANNEXE IV – Règles d'enregistrement des traits d'identité

Les règles générales suivantes sont applicables lors de l'enregistrement manuel des traits d'identités.

Nom de naissance (nom de famille)

L'enregistrement de ce trait strict est obligatoire (cf. Exi PP 02). Il doit être saisi tel qu'il apparaît sur la ligne *nom* du document d'identité, en caractères majuscules non accentués, sans signe diacritique et sans abréviation, même s'il s'agit d'une suite de « X » ou tout autre mention pour signifier que la personne n'a pas de nom. Comme c'est le cas pour l'identité INS, les traits d'union et apostrophes doivent être conservés. En revanche, les autres caractères tels que « / » doivent être remplacés par un espace.

Remarque : pour certains usagers d'origine étrangère, le titre d'identité ne précise pas le nom de naissance. Dans ce cas, le trait est enregistré « aux dires de l'usager ». Mais, comme il s'agit d'un trait strict, l'identité numérique devra rester au statut « identité provisoire » tant que cette information n'aura pas été prouvée à l'aide d'un document d'identité du pays distinguant les différents traits d'identité.

Les cas particuliers doivent faire l'objet d'une décision au cas par cas et être signalés au niveau régional voire national. Ils font également l'objet de fiches pratiques formalisées par le réseau des référents régionaux en identitovigilance (3RIV).

Une procédure interne doit décrire les modalités d'attribution d'un nom de naissance approximatif ou fictif dans les situations où il est accueilli un usager non accompagné et impossible à identifier (comateux, non communiquant, délirant) ou faisant valoir ses droits à l'anonymat.

Premier prénom de naissance

L'enregistrement de ce trait strict est obligatoire (cf. Exi PP 02).

L'état civil autorise de porter un prénom composé (exemple : Jean-Pierre) mais, comme il n'est pas obligatoire de relier les 2 parties du prénom composé par un tiret (exemple : Jean Pierre), cela peut compliquer la tâche de la personne chargée d'enregistrer l'identité numérique. Dans cette situation, il est possible de s'appuyer :

- soit sur la pièce d'identité présentée, si elle utilise une virgule pour séparer les prénoms, en enregistrant les premiers prénoms avant la première virgule, tels qu'ils apparaissent ;
- soit sur les indications de l'usager (ou de son représentant).

La prise en compte des cas particuliers (prénoms composés sans tiret de liaison, par exemple) doit faire l'objet d'une décision au cas par cas.

Une procédure interne doit décrire les modalités d'attribution d'un 1er prénom de naissance approximatif ou fictif dans les situations où il est accueilli un usager non accompagné et impossible à identifier (inconscient, non communiquant, délirant) ou faisant valoir ses droits à l'anonymat.

Prénom(s) de naissance

Ce champ fait partie des traits stricts à renseigner dès lors qu'il est possible d'accéder à un document d'identité (cf. Exi PP 03). Il doit être saisi tel qu'il apparaît sur la ligne *prénom* du document d'identité, en caractères majuscules non accentués, sans signe diacritique et sans abréviation, même s'il s'agit d'une suite de « X » ou qu'il est écrit « SP » ou « VIDE » pour signifier que la personne n'a pas de prénom. Comme c'est le cas pour l'identité INS, les tirets et apostrophes doivent être conservés mais, s'il existe des virgules séparant les prénoms sur le titre d'identité, celles-ci ne doivent pas être enregistrées.

Remarque : la liste des prénoms de l'identité INS peut comporter des prénoms composés, avec ou sans tiret de liaison, mais elle n'utilise pas de virgule pour séparer les prénoms (cf. Premier prénom de naissance).

Les cas particuliers doivent faire l'objet d'une décision au cas par cas et être signalés au niveau régional voire national. Ils font également l'objet de fiches pratiques formalisées par le réseau des référents régionaux en identitovigilance (3RIV).

Date de naissance

L'enregistrement de ce trait strict est obligatoire (cf. Exi PP 02). Il est saisi et affiché localement sous le format JJ/MM/AAAA.

Comme pour les autres traits stricts, la date de naissance à enregistrer est celle établie d'après un document ou un dispositif officiel d'identité et non celle lue sur un document de l'Assurance maladie, qui peut être différente[25]. [Exi PP 16]

Les systèmes d'information peuvent permettent de traduire dans le format JJ/MM/AAAA les dates de naissance libellées dans un calendrier luni-solaire pour les usagers nés à l'étranger. [Exi SI 15]

Lorsque la date de naissance fournie par le document d'identité ou le dispositif d'identification numérique est incomplète, il faut appliquer les consignes suivantes :

- si seul *le jour* est inconnu, il est remplacé par le premier jour du mois (01/MM/AAAA) ;
- si seul *le mois* n'est pas connu, il est remplacé par le premier mois de l'année (JJ/01/AAAA) ;
  si *le jour ET le mois* ne sont pas connus, il faut saisir la date du 31 décembre de l'année de naissance[26] (31/12/AAAA) ;
- si *l'année* n'est pas connue précisément, on utilise l'année ou la décennie estimée ;
- si la *date de naissance* est inconnue, on enregistre 31/12 et une année ou décennie compatible avec l'âge annoncé ou estimé, par exemple, 31/12/1970.

Remarque : si le système d'information le permet, un marqueur spécifique de type « Date fictive », « Date provisoire », « Date incertaine » etc. doit être utilisé pour différencier les dates de naissance réelles des cas où la date est interprétée avec les règles ci-dessus. Ce marqueur peut faire l'objet d'une transmission informatique.

Sexe

[25] L'utilisation des données de l'assurance maladie pour la facturation des soins n'est pas dans le champ du RNIV (cf. 1.2)

[26] Cette consigne n'est pas applicable pour un enfant < 1 an hospitalisé (date d'entrée de prise en charge est antérieure à la date de naissance). Il est recommandé alors d'estimer approximativement le mois de naissance (01/mm/AAAA).

L'enregistrement de ce trait strict est obligatoire (cf. Exi PP 02). Il est saisi le code du sexe (M ou F), porté sur le document d'identité lorsqu'il est présenté ; il est également possible, de façon provisoire, d'utiliser le code « I » pour *indéterminé*[27].

Remarque : Lors d'une procédure de réassignation sexuelle, la prise en compte du changement d'identité peut être décidée au niveau local en fonction d'un protocole interne. Elle peut se baser, par exemple, sur le jugement du tribunal administratif faisant apparaître l'ancienne et la nouvelle identité. L'identité doit, dans tous les cas, être remise au statut ***Identité provisoire*** pour permettre la modification des traits stricts (avec l'effacement ou l'invalidation du matricule INS s'il était enregistré). Il sera nécessaire ensuite d'attendre la présentation d'un document d'identité de haut niveau de confiance avec la nouvelle identité (cf. 3.3.3.2) pour attribuer le statut ***Identité validée*** puis, après récupération de la nouvelle identité INS via le téléservice dédié, celui d'***Identité qualifiée***.

Lieu de naissance

L'enregistrement de ce trait strict est obligatoire (cf. Exi PP 02).

Pour les personnes nées en France, il faut enregistrer le code officiel géographique (COG) de l'INSEE[28] correspondant à la commune de naissance. Pour les personnes nées à l'étranger, il faut enregistrer le code INSEE du pays (qui commence par 99)[29] et, si c'est souhaité par la structure, la ville de naissance.

Remarque : le nom de la commune de naissance (pour tous) et le code postal (pour les communes françaises) ne font pas partie des traits stricts mais peuvent être enregistrés dans des champs *ad hoc* des traits complémentaires. Dans ce cas, pour les personnes nées en France, il est souhaitable que le système d'information soit en mesure de proposer le code INSEE à partir de l'une ou l'autre de ces données, saisies de façon manuelle. Le code INSEE de la commune de naissance étant celui qui était valide à la date de naissance du patient, il peut apparaître une divergence entre le code saisi manuellement et le code renvoyé par le téléservice INSi. Dans cette circonstance, c'est le code de l'identité INS qui prévaut : il doit remplacer le précédent (cf. Annexe VI).

Si le lieu de naissance est inconnu, il faut coder 99999.

Le nom utilisé

L'enregistrement du *nom utilisé* est obligatoire lorsqu'il est différent du nom de naissance. [Exi PP 17]

Ce champ est destiné à permettre l'enregistrement du nom utilisé par l'usager dans la vie courante. Comme pour le nom de naissance, il doit être saisi en caractères majuscules non accentués, sans signe diacritique et sans abréviation mais en conservant les traits d'union et apostrophes.

S'agissant d'un trait complémentaire, cette information n'intervient pas sur le statut de l'identité numérique. Chaque structure de santé définit les règles d'alimentation de ce champ dans son système d'information, en fonction de sa politique d'identitovigilance, de ses activités, de sa

---

[27] Cela peut être le cas notamment pour des enfants de moins de 2 ans où le sexe peut être transitoirement difficile à déterminer. L'identité INS renvoyée par le téléservice INSI ne peut, quant à elle, comporter que des valeurs F ou M.

[28] https://www.INSee.fr/fr/information/2560452

[29] https://www.insee.fr/fr/information/2028273

patientèle voire des obligations contractuelles qu'elle peut avoir avec d'autres structures. Le choix peut être fait de limiter son utilisation à l'enregistrement exclusif des informations d'état civil mentionnées sur une pièce d'identité ou d'accepter d'enregistrer tout nom effectivement utilisé par l'usager (cf. 3.1.3.3). La structure peut également décider de rendre obligatoire la saisie de ce trait, même quand le nom utilisé est identique au nom de naissance.

- Lorsque le nom utilisé est le *nom d'usage* (cf. Annexe II), il correspond à celui qui est inscrit sur la ligne *nom d'usage* du titre d'identité présenté, sans la mention qui le précède telle que : « époux/se de », « divorcé/e de », « veuf/ve », leur abréviation sur les titres français (« Ep. », « Div. », « Vve ») ou leur équivalent sur les titres étrangers.

  Remarque : l'utilisation effective du nom d'usage mentionné sur la pièce d'identité peut changer à l'occasion d'événements d'état civil (mariage, divorce…). Il appartient à la structure d'évaluer la pertinence de prendre en compte les modifications non officialisées et/ou d'inviter l'usager à faire mettre à jour son titre d'identité auprès des services d'état civil[30].

- Lorsque le nom utilisé est le *nom de naissance* – si la structure a fait le choix d'alimenter le champ dans cette situation – sa recopie à partir du champ *nom de naissance*, par action volontaire de l'utilisateur, peut utilement être facilitée par le système d'information.

- Pour des personnes n'employant pas leur nom de naissance au complet dans la vie courante, l'enregistrement peut être limité à la partie du nom effectivement utilisée (exemple fictif : pour M. SAINT JOUAN DE LA FRAIRIE, qui n'utilise dans la vie courante que la première partie de son nom (SAINT JOUAN), seule celle-ci sera enregistrée).

- Ce champ peut aussi servir à enregistrer la partie nom du *pseudonyme* ou du *surnom* (cf. Annexe II), à la triple condition que ce soit : (1) sur demande expresse de l'usager ; (2) un trait constant, utilisé à chaque venue ; (3) une pratique autorisée par la politique d'identitovigilance de la structure.

Le prénom utilisé

L'enregistrement du *prénom utilisé* est obligatoire lorsqu'il est différent du *premier prénom de naissance*. [Exi PP 18]

Ce champ est destiné à permettre l'enregistrement du prénom utilisé par l'usager dans la vie courante. Comme pour les prénoms de naissance, il doit être saisi en caractères majuscules non accentués, sans signe diacritique et sans abréviation mais en conservant les traits d'union et apostrophes.

S'agissant d'un trait complémentaire, cette information n'intervient pas sur le statut de l'identité numérique. Chaque structure de santé définit les règles d'alimentation de ce champ dans son système d'information, en fonction de sa politique d'identitovigilance, de ses activités, de sa patientèle voire des obligations contractuelles qu'elle peut avoir avec d'autres structures. Le choix peut être fait de limiter son utilisation à l'enregistrement exclusif des informations d'état civil mentionnées sur une pièce d'identité ou d'accepter d'enregistrer tout prénom effectivement utilisé par l'usager (cf. 3.1.3.3). La structure peut également décider de rendre obligatoire la saisie de ce trait même quand le prénom utilisé est identique au premier prénom de naissance.

---

[30] https://www.service-public.fr/particuliers/vosdroits/R19902

- Lorsque le prénom utilisé est un des *prénoms de naissance*[31], l'alimentation de ce champ peut utilement être facilitée par le système d'information en proposant la recopie, par action volontaire de l'utilisateur, de tout ou partie du champ *prénom(s) de naissance* ou du *premier prénom de naissance*.
- Lorsque le prénom utilisé est le *prénom usuel* (cf. Annexe II) officiellement déclaré à l'état civil, il correspond à celui qui est inscrit sur la ligne *ad hoc* du titre d'identité présenté.
- Ce champ peut aussi servir à enregistrer tout prénom couramment utilisé par l'usager sans avoir été officialisé ou faisant partie de son *pseudonyme* ou de son *surnom* officiel (cf. Annexe II), à la triple condition que ce soit : (1) sur demande expresse de l'usager, (2) un trait constant, utilisé à chaque venue, (3) une pratique autorisée par la politique d'identitovigilance de la structure.

[31] Article 57 du code civil

ANNEXE V – Identification primaire sans présence physique de l'usager

Le développement de la télémédecine, de l'utilisation d'outils d'inscription à distance et d'applications facilitant la coordination de la prise en charge de l'usager par plusieurs professionnels de santé augmente le nombre de situations particulières d'identification. La transmission d'informations de santé par voie informatique et la mise en application des règles concernant l'usage du matricule INS nécessitent la mise en œuvre de conditions particulières de sécurisation de l'identification primaire par les structures réalisant des actes sans présence physique de l'usager.

Réalisation d'actes pour le compte d'un tiers, sans lien direct avec l'usager

Lorsqu'une structure prestataire de service est chargée de réaliser des actes sur demande d'un autre professionnel (« prescripteur ») sans être en mesure de vérifier l'identité de l'usager pour lequel elle réalise la prestation, du fait de l'absence de ce dernier, la responsabilité de l'identification primaire repose sur la structure émettrice de la demande (cf. 3.1.2.3). C'est le cas, par exemple, pour :

- les laboratoires de biologie médicale et d'anatomie et de cytologie pathologiques ;
- l'établissement français du sang (EFS) et le Centre de transfusion sanguine des armées (CTSA) ;
- la réalisation d'expertises professionnelles telles que les réunions de concertation pluridisciplinaire (RCP) réalisées alors que le patient n'est pas connu par la structure organisatrice ;
- la demande de coordination de parcours de santé adressée par un acteur de santé.

Plusieurs cas de figures peuvent être distingués, en fonction de l'existence d'un enregistrement précédent de l'usager, de son statut et de la confiance que le prestataire accorde au prescripteur sur la qualité de l'identité adressée.

Le prestataire a toute confiance dans la qualité de l'identité adressée

Le prescripteur et le prestataire sont normalement liés par un contrat qui garantit, entre autres, la qualité des procédures d'identitovigilance du prescripteur. Dans ce cas, le prestataire qui reçoit une identité numérique peut, par dérogation à la règle générale, la considérer comme :

- *Identité qualifiée* lorsque celle-ci est transmise avec le matricule INS et le qualificatif « validé » dans le message d'interopérabilité, même en l'absence de possibilité de vérification par le téléservice INSi (cas dérogatoire à la règle qui reste la procédure à privilégier) ;
- *Identité validée* lorsque celle-ci est transmise sans matricule INS avec le qualificatif « validé » dans le message d'interopérabilité ;
- *Identité provisoire* dans les autres cas.

Dans le cas où l'identité n'est pas reçue sous format dématérialisé, l'appel au téléservice est obligatoire si l'identité n'est pas connue du prestataire ou ne dispose pas d'un statut récupéré ou qualifié (cf. 4.2.3.2 et Exi PP 01).

Si l'usager n'est pas encore connu du prestataire, il crée une identité numérique en utilisant les traits et le statut déduit de la transmission par le prescripteur.

Si une identité numérique locale correspondante est déjà enregistrée avec un statut I*dentité validée* ou *Identité qualifiée* :

- la réception d'une *identité validée* ou *qualifiée* autorise l'alimentation directe du dossier local de l'usager ;
- dans le cas où l'identité est transmise avec un niveau de confiance inférieur et que le prestataire n'est pas en situation de lever le doute (par contact avec le prescripteur, par exemple), il ne faut pas prendre le risque de créer une collision mais créer une nouvelle identité numérique comme cela serait fait pour un usager d'identité approchante (en utilisation l'attribut *Identité homonyme* s'il est disponible).

Le prestataire ne doit pas propager auprès d'autres correspondants le matricule INS transmis par le prescripteur en dehors du cas où l'identité numérique locale bénéficie du statut identité qualifiée.

Le prestataire ne peut pas garantir la qualité de l'identité adressée

Lorsque le prescripteur est inconnu du prestataire ou que la qualité de ses pratiques d'identitovigilance n'est pas assurée par contrat, les consignes dérogatoires du chapitre précédent ne peuvent être appliquées. La prise en compte de l'identité transmise doit suivre les règles communes en vigueur qui interdisent de valider les traits sans possibilité de contrôle de cohérence à partir d'un dispositif d'identité et d'enregistrer le matricule INS sans appel au téléservice de vérification (cf. 3.1.2.3).

Comme le prestataire n'est pas en mesure de qualifier l'identité numérique, il ne doit pas propager auprès d'autres correspondants le matricule INS transmis par le prescripteur.

Réalisation d'un acte avec un usager présent à distance (télémédecine)

L'usage d'outils de télémédecine est appelé à devenir plus fréquent du fait du développement du numérique en santé. La télémédecine concerne la réalisation d'actes à distance :

- pour réaliser un examen clinique ou technique (téléconsultation, télédiagnostic, téléimagerie, télésurveillance…) ;
- pour échanger des avis entre professionnels de santé (télé-expertise).

Le recueil et la validation de l'identité à distance, en l'absence d'un professionnel à ses côtés, nécessite plusieurs conditions :

- le recueil et l'enregistrement de son identité numérique (éventuellement réalisé par le biais d'un dispositif numérique d'identification électronique certifié substantiel eIDAS, cf. 3.3.3.2) ;
- le contrôle de cohérence entre l'identité numérique et celle de l'usager physique le jour de la consultation.

Lorsque l'usager est accompagné d'un professionnel aidant, l'attestation de son identité réelle est confiée à ce dernier. Dans le cas contraire, il peut être nécessaire de se servir d'outils d'authentification dédiés ou, lorsque c'est possible, de demander à l'usager de présenter son titre d'identité à la caméra.

Lorsqu'une création d'identité numérique est nécessaire pour un usager non connu, un appel au téléservice INSi peut être réalisé par la structure afin de récupérer une identité INS et d'attribuer un niveau de confiance correspondant.

Il est indispensable d'utiliser de bonnes pratiques de recherche de l'antériorité des dossiers (cf. 3.1.1). C'est notamment le cas dans des situations où l'accès aux images et comptes rendus

est autorisé par le biais d'un portail aux professionnels de santé engagés dans la prise en charge d'un usager (médecin traitant, spécialiste, équipe participant à une réunion de concertation pluridisciplinaire…). Ces pratiques sont encadrées par une procédure *ad hoc*.

Exemple de la téléimagerie

La téléimagerie (en radiologie et médecine nucléaire) est un acte de télémédecine qui permet à un spécialiste de consulter des images à distance[32] dans l'objectif :

- soit d'interpréter un examen réalisé sur un autre site, en lien avec des professionnels au contact direct du patient (médecin demandeur, manipulateur d'électroradiologie médicale chargé de l'acte technique…) ;
- soit d'échanger un avis avec un confrère de la même spécialité qui le sollicite sur un cas particulier.

Le dialogue direct entre les professionnels, obligatoire dans ce type d'activité, est censé faciliter l'étape d'identification de l'usager. Quelle que soit l'urgence, celle-ci repose sur la structure à l'origine de la demande. Les parties prenantes doivent s'assurer que l'examen – interprétation et archivage des images – est bien identifié avec les traits connus de la personne examinée.

Que ce soit pour la création d'un nouveau dossier ou dans le cas où l'usager disposait déjà d'une identité numérique dans le système d'information – sous réserve de la cohérence des traits fournis avec les données préalablement enregistrées – le statut de l'identité numérique locale est attribué en fonction de plusieurs paramètres :

- *identité qualifiée* si l'identité INS est fournie OU que ce statut était déjà attribué localement OU que le contrôle de cohérence atteste que l'identité correspond bien à une identité locale préalablement enregistrée comme *Identité récupérée* ;
- *identité validée* si le contrôle de cohérence entre les jeux d'identité est bien réalisé ou que ce statut préexistait ;
- *identité récupérée* si ce statut préexistait et que le contrôle de cohérence n'est pas réalisé ;
- *identité provisoire* dans les autres cas.

Dans tous les cas, il est nécessaire que cette pratique soit encadrée par une convention de partenariat qui précise notamment les modalités techniques des échanges informatiques afin de garantir leur sécurité. Elle doit notamment préciser le cas où :

- le prestataire a l'autorisation de se connecter au système d'information de l'imagerie de la structure requérante (PACS[33]), ce qui lui permet d'interpréter directement les images dans celui-ci après s'être assuré d'être connecté sur le bon dossier ;
- la connexion n'est pas directe ou fait appel à une iconographie partagée (exemple : utilisation d'une plateforme territoriale ou régionale dédiée), ce qui nécessite d'appliquer strictement les règles de recherche des dossiers antérieurs afin de ne pas risquer une erreur de personne (cf. 3.1.1).

Inscription à distance d'un usager

Il existe de plus en plus de situations où l'identification primaire de l'usager est réalisée par l'intermédiaire d'une solutions amont de prise de rendez-vous/pré-consultation/pré-admission au

---

[32] HAS. Fiche mémo télé-imagerie mai 2019 (https://www.has-sante.fr/upload/docs/application/pdf/2019-07/fiche_memo_teleimagerie.pdf)

[33] *Picture Archiving and Communication System* (système d'archivage et de transmission d'images)

sein d'un portail patient en ligne mettant à contribution l'usager pour la gestion de son identité numérique. Ce type de solution s'apparente à un référentiel d'identités basé sur un domaine d'identification différent de celui de la structure/du professionnel, puisque les identités qu'il contient sont créées/mises à jour à l'initiative de l'usager lui-même.

Dans ces solutions de prise de rendez-vous/pré-consultation/pré-admission au sein d'un portail patient en ligne, une identité peut acquérir le statut *identité qualifiée*, si l'inscription de l'usager a été accompagnée d'une vérification de son identité par l'intermédiaire d'un dispositif d'identification électronique certifié substantiel eIDASet de l'appel au téléservice INSi. Dans ce cas, l'ensemble de l'identité INS (dont le matricule INS et son OID) peut être transmis vers le SIS. La requalification de cette identité dans le domaine d'identification de l'établissement n'est pas nécessaire quand les deux domaines d'identification (amont et référentiel patient de l'établissement) sont portés par la même personne morale.

À défaut du statut *identité qualifiée*, le matricule INS (et son OID) ne sont pas transmis vers le SIS : seuls les traits sont transmis (éventuellement récupérés par l'intermédiaire du téléservice INSi).

L'inscription via un dispositif numérique d'identification électronique certifié substantiel eIDAS (cf. 3.3.3.2) permet de sécuriser l'identité numérique créée, sous réserve que les traits attendus par le système d'information soient effectivement renseignés lors de la procédure mais il ne permet pas de s'assurer que la personne enregistrée est bien celle qui sera prise en charge. Il n'est donc pas possible de valider une identité numérique créée à distance avant de s'être assuré que l'usager inscrit est bien celui qui bénéficie de la prestation. L'identité numérique recueillie, très incomplète, ne peut donc être qu'au statut *Identité provisoire*[34].

Il appartient à la structure de mettre en œuvre les bonnes pratiques d'identitovigilance, lors de la venue effective de l'usager, afin de compléter les données, de les rattacher à un dossier existant si l'usager était déjà connu et de faire évoluer en conséquence le statut de l'identité numérique (cf. 3.3.1).

[34] Voire d'une identité au statut *Identité récupérée* si les outils évoluent, permettant l'interrogation du téléservice INSi de récupération

ANNEXE VI – Évaluation de la cohérence de l'identité INS

- Quand est-il nécessaire d'évaluer cette cohérence ?

  Les différentes situations où il est nécessaire d'évaluer la cohérence entre les traits de l'identité INS et ceux relevées localement sont les suivantes :
  - la création d'une identité par l'intermédiaire du téléservice (cf. 3.1.2.1) ;
  - l'appel au téléservice de récupération alors qu'une identité numérique a déjà été créée localement (cf. 3.1.2.2 et 3.1.2.3) ;
  - l'échec d'une opération de vérification d'une identité qualifiée (cf. 4.2.3.2 et 4.2.3.4) ;
  - la réception de données de santé transmises par un acteur de santé externe à la structure (cf. 3.1.2.3).

- Pourquoi cette évaluation est-elle nécessaire ?

  Dans le cas de la récupération de l'identité INS, l'objectif est de vérifier que les traits proposés par le téléservice INSi correspondent bien à ceux de l'identité recherchée avant d'accepter de les enregistrer dans le système d'information local.

  Dans le cas de la vérification de l'identité INS, l'objectif est de ne pas transmettre une identité INS invalide avant d'avoir recherché l'origine de l'échec de la vérification.

  Dans le cas de la réception de données de santé, l'objectif est de ne pas intégrer des informations qui pourraient appartenir à un autre patient (collision).

- Quelles sont les sources de divergences potentielles ?

  L'absence de cohérence entre les traits de référence portés par l'identité INS et les informations locales peuvent avoir différentes sources :
  - une origine locale, qui peut être en lien avec une erreur de saisie manuelle des traits (inversion de lettre…), l'emploi d'anciennes règles de saisie, sans oublier l'erreur de sélection du dossier avant appel du téléservice ou du bénéficiaire concerné sur la carte Vitale, lorsque l'appel est réalisé par ce biais ;
  - des différences qui peuvent exister entre le titre d'identité et l'identité présente dans le *Répertoire national d'identification des personnes physiques* (RNIPP), du fait de règles d'état civil spécifiques à chacun des domaines ou de l'utilisation de virgules pour séparer les prénoms ;
  - l'erreur d'identification de l'usager avant la transmission de données de santé par un acteur de santé.

- Quelle est la conduite à tenir en cas de constat d'anomalie ?

  En fonction de la nature de la divergence constatée, il pourra être décidé :
  - de valider les différences acceptables : l'ensemble des traits de l'identité INS deviennent alors ceux à utiliser comme traits stricts (cf. Exi SI 12 et Exi PP 11) ;
  - de refuser l'identité présentée par le téléservice et donc de conserver les traits saisis localement[35] ;

[35] **L'identité présente sur un dispositif d'identité à haut niveau de confiance prime sur toutes les autres**

- de rechercher l'origine du problème, notamment quand il est constaté *a posteriori* des différences notables entre l'identité récupérée par le biais du téléservice et la pièce d'identité à haut niveau de confiance présentée pour valider l'identité numérique ;
- de faire évoluer le statut de l'identité numérique en conséquence (cf. Annexe VII) ;
- de ne pas intégrer automatiquement les données de santé transmises par un autre acteur de santé s'il existe un doute quant à l'identité associée (risque de collision).

- Comment organiser cette recherche de cohérence ?

  Le contrôle de cohérence est effectué à l'occasion d'une venue de l'usager, de préférence en présence de celui-ci, ou de la réception de données le concernant (titre d'identité pour la mise à jour des données, données de santé transmises par un tiers).

  Lorsque les traits INS provenant du téléservice sont acceptés, l'identité enregistrée prend alors le statut d'*Identité qualifiée* (hors attributs *identité fictive* et *identité douteuse*) – lorsque la validation de l'identité est réalisable sur le moment – ou d'*Identité récupérée* dans le cas contraire.

  L'opération de qualification doit parfois être différée. C'est le cas par exemple lorsque le flux des usagers à accueillir est trop important ou que la multiplication des tâches ne permet pas d'assurer le niveau de vigilance nécessaire. Elle peut alors être réalisée « en *backoffice* » par des professionnels dédiés de la structure, à condition que l'identité de l'usager ait été vérifiée lors de l'accueil physique et que la procédure prévoie de pouvoir s'appuyer sur la pièce d'identité ayant servi à créer ou modifier le dossier de l'usager ; ce qui impose qu'elle soit sauvegardée par photocopie ou numérisation[36].

  Il appartient aux instances locales d'identitovigilance de formaliser sous forme de procédure(s) – applicable(s) à tout ou partie de la structure – par qui et comment est réalisée l'évaluation de la cohérence (entre les traits de la pièce d'identité ou de l'identité numérique locale et ceux renvoyés par le téléservice INSi et/ou transmis avec des données de santé). Un document qualité *ad hoc* doit aussi prévoir la conduite à tenir en fonction des résultats des opérations périodiques de vérification des identités qualifiées du référentiel d'identités (cf. 4.2.3).

- Comment gérer la divergence entre les jeux de traits ?

  Les principales sources d'incohérences connues à ce jour, en lien avec la nature des informations renvoyées par le téléservice INSi, portent sur :
  - l'existence de données vides dans les champs de certains usagers, essentiellement ceux nés à l'étranger (cf. 3.2.1.1) ;
  - la date de naissance qui peut être dans un format inhabituel en renvoyant des valeurs nulles à la place des jours et/ou des mois (cf. 3.2.1.1) ;
  - le lieu de naissance, qui utilise le code INSEE de la commune qui existait lors de l'inscription au RNIPP mais qui peut avoir changé dans l'intervalle (ce qui n'est pas une véritable incohérence).

  Lorsque l'incohérence des traits transmis avec les données locales est jugée trop importante, elle justifie de ne pas récupérer l'identité INS et/ou de ne pas intégrer dans le dossier de l'usager les données de santé reçues. Il n'est pas possible de lister de façon exhaustive

[36] Sous réserve du respect des règles de conservation des données en vigueur

l'ensemble des situations : elles sont le plus souvent à gérer au cas par cas et validées collectivement, en tenant compte des procédures applicables localement.

Exemples :

- S'il s'avère que la divergence est en rapport avec une erreur de saisie locale[37], l'identité INS est acceptée au statut *Identité récupérée* ou – après validation de l'identité – *Identité qualifiée*.
- Si les différences sont mineures et jugées acceptables, la priorité est à donner à l'identité INS. Exemples : code INSEE de la commune de naissance différent mais relatif à la même commune ; prénoms affichés de façon distincte mais cohérents avec la pièce d'identité ; anomalie en lien avec la présence de traits d'union et apostrophes dans un seul des 2 jeux de traits ; date de naissance transmise différente d'une date de naissance locale interprétée (cf. Annexe IV)…
- Lorsque l'incohérence est liée à une erreur sur la pièce d'identité, confirmée par l'usager, il faut inviter l'usager (ou ses proches) à la faire corriger auprès de l'état civil[38].
- Lorsque les différences sont plus importantes et semblent révéler une erreur au niveau de la base nationale de référence (exemple : date de naissance incohérente par rapport au document d'identité de haut niveau de preuve présenté localement, erreur d'écriture du nom ou d'un prénom…), il est préférable de ne pas récupérer l'identité INS ; il faut alors inviter l'usager (ou un proche) à adresser une demande de correction d'état civil à l'INSEE[39] en joignant une copie intégrale d'acte de naissance.
- Lorsque l'identité transmise par un autre acteur de santé est mise en doute, il faut prendre contact directement avec la personne à la source de la transmission pour effectuer les vérifications nécessaires.

Remarque : même dans les cas où l'identité numérique a été créée avec l'identité INS récupérée, la mise en évidence *a posteriori* de divergences non mineures avec le document d'identité à haut niveau de confiance doit empêcher l'opération de qualification. Il peut même s'avérer nécessaire, puisque l'identité INS n'est pas modifiable, de déclasser l'identité numérique en *Identité provisoire* (cf. Annexe VII) de façon à corriger manuellement les traits pour les rendre conformes à ceux de la pièce d'identité de haut niveau de preuve – ce qui doit entraîner automatiquement la suppression (ou l'invalidation) du matricule INS initialement associé.

- Comment signaler les anomalies rencontrées ?

  Il est important que toute difficulté rencontrée pour la récupération de l'identité INS ou la qualification de l'identité numérique, du fait d'une incohérence non mineure, soit signalée comme événement indésirable et rapportée au niveau régional et national. [Reco PP 02]

[37] Les éléments en discordance peuvent, dans ce cas, être mis en évidence par le système d'information

[38] https://www.service-public.fr/particuliers/vosdroits/R19902

[39] https://psl.service-public.fr/mademarche/rnipp/demarche?execution=e1s1

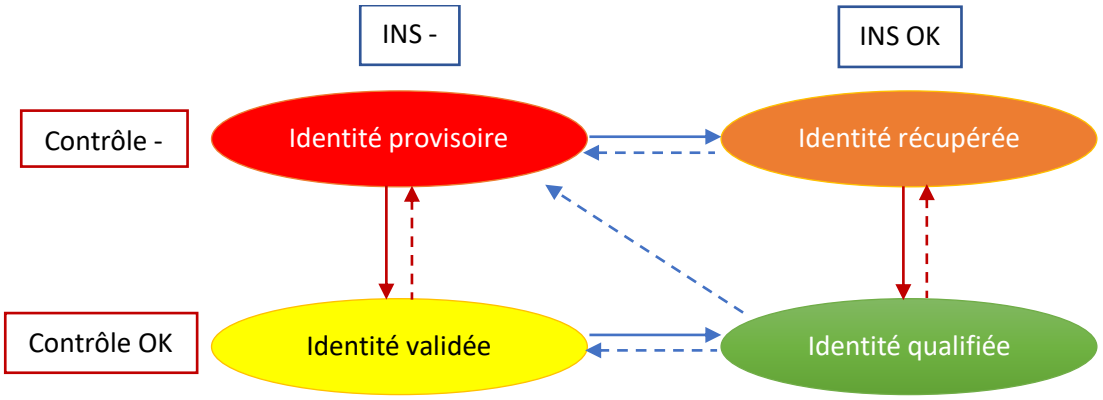
ANNEXE VII – Statuts de l'identité numérique locale

- Modalités d'attribution du statut en fonction du mode de création de l'identité numérique

Etape 1	Identité numérique existante ?	Document d'identité de confiance ?	Statut de confiance initial	Etape 2	Identité renvoyée par INSi ?	Traits cohérents et acceptés ?	Statut de confiance final	Traits stricts enregistrés	Utilisation matricule INS ?
Accueil de l'usager	Non	Non		Interrogation TLS INSi	Non		Identité provisoire	Ceux saisis localement	Non
		Oui			Oui	Oui	Identité récupérée	Ceux de l'INS	Locale
	Oui	Non	Identité provisoire		Non		Identité validée	Ceux saisis localement	Non
					Oui	Oui	Identité qualifiée	Ceux de l'INS	Oui
					Non		Identité provisoire	Ceux saisis localement	Non
					Oui	Non			
						Oui	Identité récupérée	Ceux de l'INS	Locale
		Oui	Identité validée		Non		Identité validée	Ceux saisis localement	Non
					Oui	Non	Identité validée ou Identité provisoire*	Incohérence à gérer par la structure (cf. Annexe 4)	Non
						Oui	Identité qualifiée	Ceux de l'INS	Oui

** selon le choix de la structure.*

- Évolutions possibles des statuts



Il est possible de faire évoluer favorablement le statut de confiance :

- de *provisoire* à *validée* ou de *récupérée* à *qualifiée* après contrôle de cohérence satisfaisant entre l'identité numérique et celle de l'usager relevée à partir d'un dispositif d'identité à haut niveau de confiance (cf. 3.3.3.2) ;
- de *provisoire* à *récupérée* ou de *validée* à *qualifiée* après récupération des traits du téléservice INSi, attestant de leur cohérence avec l'identité numérique locale (cf. 3.2.1).

À l'inverse, la confiance est susceptible d'être dégradée dans certaines circonstances :

- une identité *récupérée* ou *validée* ou *qualifiée* qui s'avère secondairement être en lien avec l'utilisation frauduleuse d'une carte Vitale doit faire l'objet d'un déclassement en Identité *provisoire* avec utilisation de l'attribut *Identité douteuse* (cf. 3.3.2) ;

- une incohérence avec l'identité INS renvoyée par le téléservice INSi lors d'une opération de récupération d'une identité préalablement *validée* peut, si c'est le choix de la structure, entraîner le déclassement au statut Identité *provisoire*, tant que la cause de l'anomalie n'est pas identifiée et corrigée (cf. Annexe VI) ;
- en cas d'échec d'une opération de vérification à partir du téléservice INSi, l'identité numérique concernée ne peut pas rester au statut Identité *qualifiée* et le matricule INS doit être effacé ou invalidé (cf. 4.2.3.4), en alimentant une liste d'anomalies à destination de l'instance opérationnelle d'identitovigilance.

ANNEXE VIII – Affichage des traits d'identité

- Principes

Les traits d'identités affichés conformément à la réglementation doivent pouvoir être facilement distingués, sans risque d'équivoque, par les acteurs concernés (Exi SI 11).

Il doit être retrouvé *a minima* les traits stricts suivants sur les documents comportant des données d'information de santé : nom de naissance, 1er prénom de naissance, date de naissance, sexe et – si l'identité est qualifiée – matricule INS suivi de sa nature (NIR ou NIA) (Exi PP 10).

Sur une interface homme machine (IHM) ou une étiquette, ils peuvent se limiter aux traits : nom de naissance, 1er prénom de naissance, date de naissance et sexe (Exi PP 10).

Il est recommandé d'y ajouter, si applicable, les informations relatives aux nom et prénom utilisés et, si besoin, à l'identifiant local de référence (exemple : IPP).

Il est possible d'afficher la nature de chaque trait de façon explicite ou abrégée en utilisant les exemples suivants :

Trait	*Nature explicite*	*Nature abrégée*
Nom de naissance	Nom naissance :	N.Nais :
Date de naissance	Date naissance :	DDN :
Code du lieu naissance	Code lieu naissance	INSEE.Nais. :
Sexe	Sexe :	S :
Prénoms de naissance	Prénom(s) :	Pr.Nais. :
1er prénom de naissance	1er prénom :	Pr.1 :
Nom utilisé	Nom utilisé :	N.Ut :
Prénom utilisé	Prénom utilisé :	Pr.Ut. :
Matricule INS	Mat INS :	INS :
Identifiant patient	ID patient :	IPP :

D'autres alternatives peuvent être utilisées par les structures, sous réserve qu'il ne puisse exister aucun doute dans l'interprétation des données affichées par les différents correspondants. Par exemple :

- utiliser une casse différente pour l'affichage des noms et des prénoms (exemple : DARK Jeanne) ;
- séparer le premier prénom des autres prénoms de naissance par des crochets ou des parenthèses ;
- afficher les traits complémentaires, tels que nom et prénom utilisés, entre parenthèses ;
- de faire précéder le nom de naissance par *né(e)* ;
- utiliser un affichage en tableau (cf. exemples) ;
- etc.

Lorsque le matricule INS est imprimé, il n'est pas pertinent d'imprimer l'OID mais la nature du trait (NIR ou NIA) doit être précisée afin que l'outil informatique du destinataire puisse être en mesure de faire appel au téléservice INSi pour vérification.

Remarque : si tous les caractères du nom et des prénoms de naissance ne peuvent être affichés, il est nécessaire de le signaler par un astérisque (*) à la fin de la chaîne de caractères affichés.

En complément de l'identité INS « en clair », l'affichage d'un datamatrix est prévu.

- Exemples d'affichage

Les exemples suivants sont donnés à titre illustratif en reprenant les traits de la personne fictive citée aux § 3.1.3.1 et 3.1.3.3 – Mme JEANNE, MARIE, CECILE DARK veuve LOUIS – et en y ajoutant l'identifiant interne de la structure (IPP = 165487).

- Étiquettes
    - *Exemple 1 : N.Nais*: DARK *Pr.Nais*: JEANNE MARIE CECILE *S*: F *DDN*: 30/05/1960 *IPP*: 165487
    - Exemple 2 : Mme Jeanne [Marie Cecile] DARK, né(e) le 30/05/1960, appelé(e) DARK MARIE-CECILE,
      IPP: 165487
    - Exemple 3 :

N. nais	*Prénom(s)*	*S*	*DDN*	*Lieu nais.*	*Identité utilisée*	*IPP*
DARK	JEANNE (MARIE CECILE)	F	30/05/1960	88154	DARK Marie-Cecile	165487

Dans le cas dérogatoire de l'identification des prélèvements biologiques, si un système permettant de relier de façon fiable un identifiant à l'identité de l'usager prélevé est utilisé par le préleveur, les traits d'identités peuvent ne pas figurer sur l'étiquette présente sur le tube.

Plus généralement, en complément d'un affichage « en clair », les identités INS sont présentées sous forme d'un datamatrix.

- Demande d'examen :

  Nom de naissance : DARK
  Prénom(s) : JEANNE MARIE CECILE
  1er prénom de naissance : JEANNE
  Sexe : F
  Date de naissance : 30/05/1960 (INSEE : 88154)
  IPP : 165487
  INS : *260058815400233 (NIR)*

- Lettre de liaison :

  Nom de naissance : DARK
  Prénom(s) : JEANNE [MARIE CECILE]
  Née le 30/05/1960 à Domrémy-la Pucelle (INSEE : 88154)
  Sexe : F
  INS : *260058815400233 (NIR)*
  Nom et prénom utilisés : DARK Marie-Cécile

- Écran d'ordinateur *(bandeau en haut ou en bas de chaque page du dossier de l'usager)*

DARK JEANNE MARIE CECILE *né(e) le* 30/05/1960 (F) - **(qualifiée)** - *Id. utilisée: DARK Marie-Cecile*

ANNEXE IX – Glossaire des sigles utilisés

CNAM : Caisse nationale d'assurance maladie
CNAV : Caisse Nationale d'Assurance Vieillesse
COG : Code officiel géographique (codage INSEE des communes françaises)
COM : Collectivité d'Outre-mer
CPx : Carte de professionnel de santé (CPS) ou d'établissement (CPE)
CTSA : Centre de transfusion sanguine des armées
DI : Domaine d'identification
DMP : Dossier médical partagé
DOM : Département d'Outre-mer
DP : Dossier pharmaceutique
DR : Domaine de rapprochement
EFS : Établissement français du sang
eIDAS : *Electronic Identification, Authentication and Trust Services* (règlement européen pour accroitre la confiance dans les transactions électroniques)
Exi : Exigences rendues opposables par le RNIV
GDR : Gestion des risques
GHT : Groupement hospitalier de territoire
HAS : Haute autorité de santé
IHM : Interface homme machine
INS : Identité nationale de santé
INS-C : INS calculé
INSi : Téléservice de recherche et de vérification de l'identité INS
INSEE : Institut National de la Statistique et des Études Économiques
IPP : Identifiant permanent du patient (identifiant utilisé dans les SIH)
NIA : Numéro d'immaticulation d'Attente
NIR : Numéro d'Identification au Répertoire des Personnes Physiques
OID : *Object identifier* (identifiants universels utilisés pour assurer l'interopérabilité entre logiciels)
PACS : *Picture Archiving and Communication System* (système d'archivage et de transmission d'images)
POM : Pays d'Outre-mer (Nouvelle-Calédonie, Polynésie française)
PP : Pratiques professionnelles
Reco : Recommandations de bonne pratique du RNIV
RCP : Réunion de concertation pluriprofessionnelle
REX : Retour d'expérience
RGPD : Règlement général de protection des données
RNIPP : Répertoire national d'identification des personnes physiques
RNIV : Référentiel national d'identitovigilance
SNGI : Service National de Gestion des Identités
SI : Système d'information
SIH : Systèmes d'informations hospitaliers
SIS : Système d'information en santé

ANNEXE X – Références réglementaires

- Circulaire du 28 juin 1986 relative à la mise en œuvre de l'article 43 de la loi n° 65-1372 du 23 décembre 1985.
- Loi n° 2002-304 du 4 mars 2002 relative au nom de famille
- Instruction générale relative à l'état civil du 2 novembre 2004
- Article 57 du Code Civil (modifié par Ordonnance n° 2005-759 du 4 juillet 2005)
- Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (dispositions réglementaires).
- Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires).
- Circulaire n° INT/D/00/00001/C du 10 janvier 2009 relative à l'établissement et la délivrance des cartes nationales d'identité.
- Circulaire du 28 octobre 2011 relative aux règles particulières à divers actes de l'état civil relatifs à la naissance et à la filiation
- Circulaire n° 5575/SG du 21 février 2012 relatif à la civilité Mademoiselle, du nom de jeune fille, nom patronyme et nom d'épouse
- Loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité
- Loi n°2013-404 du 17 mai 2013 ouvrant le mariage aux couples de même sexe.
- Règlement 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;
- Règlement d'exécution 2015/1502 du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement 910/2014 ;
- Règlement (UE) 2016/679 du parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données [RGPD])
- Décret n°2017-412 du 27 mars 2017 relatif à l'utilisation du NIR
- Guide méthodologique Mise en œuvre de l'identité patient au sein des groupements hospitaliers de territoire (ASIP Santé, 2018)
- Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (articles L110-4-1 et L110-4-2 du code de la santé publique)
- Arrêté du 24 décembre 2019 portant approbation du référentiel « Identifiant National de Santé »
- Guide méthodologique de production des informations relatives à l'activité médicale et à sa facturation en médecine, chirurgie, obstétrique et odontologie. ATIH (mise à jour annuelle).
- Manuel de certification des établissements de santé (version 2014 ou 2020)
- Nomenclature des communes et des pays et territoires étrangers INSEE
- Normes ISO (9001, 15189…)
- CI-SIS (https://esante.gouv.fr/interoperabilite/ci-sis)
- https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/referentiel-documentaire-lie-au-reglement-eidas/

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

Liberté
Égalité
Fraternité