L'identitovigilance en 2021

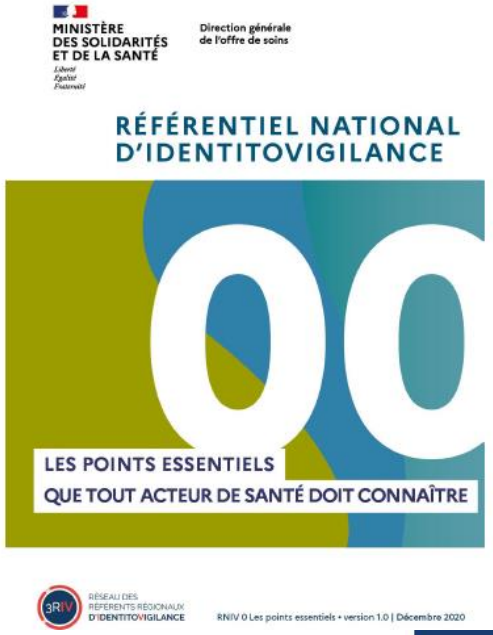
Les principes clés d'identification définies

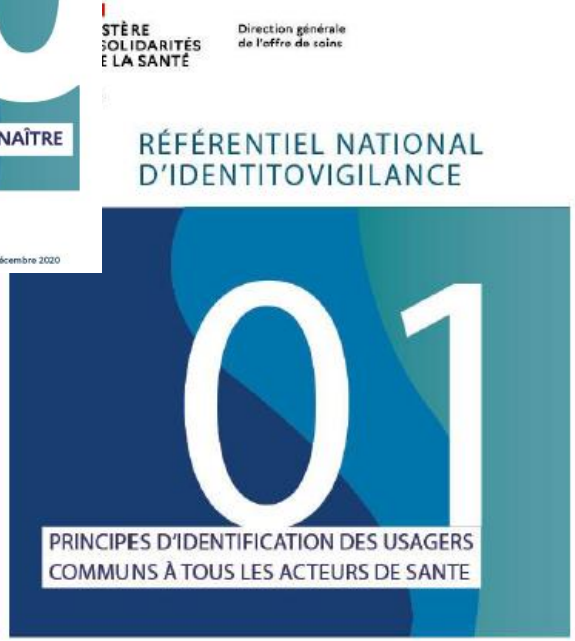
par l'Identifiant National de Santé INS,

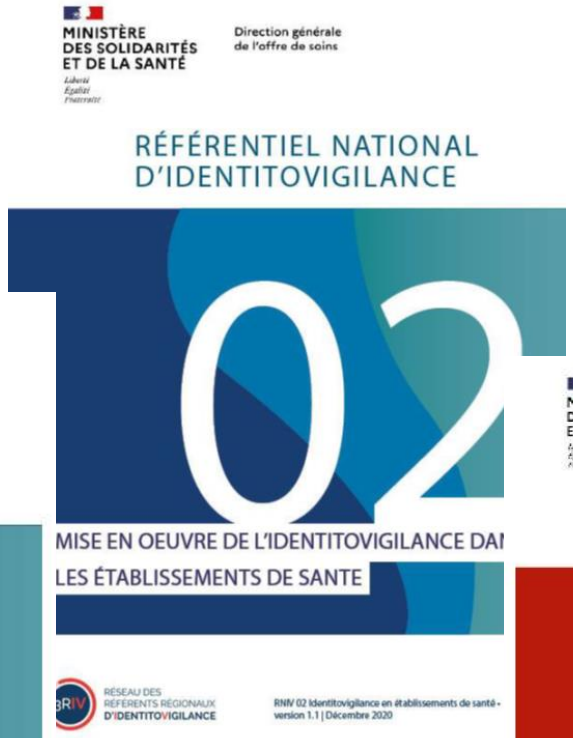
le référentiel national d'identitovigilance RNIV 1,

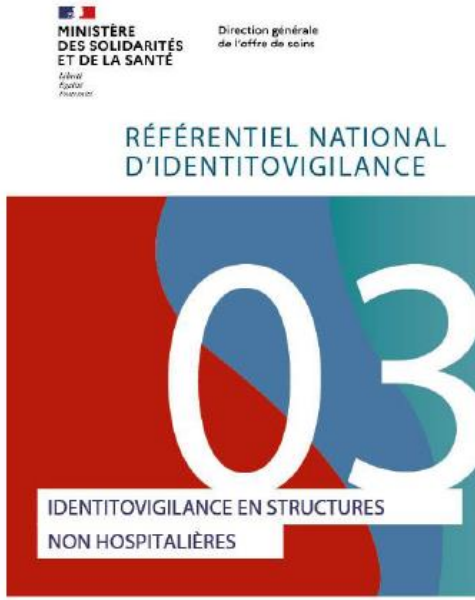
et la mise en oeuvre dans les établissements de santé RNIV 2

Référentiels nationaux actuellement disponibles



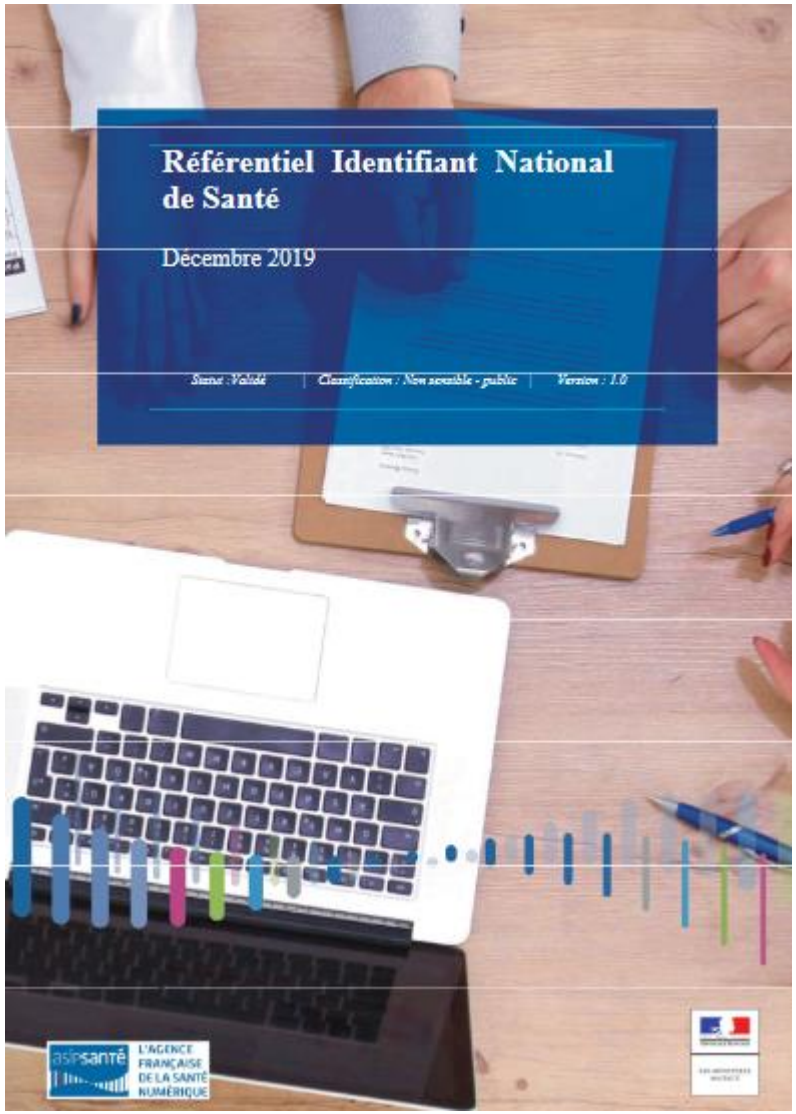




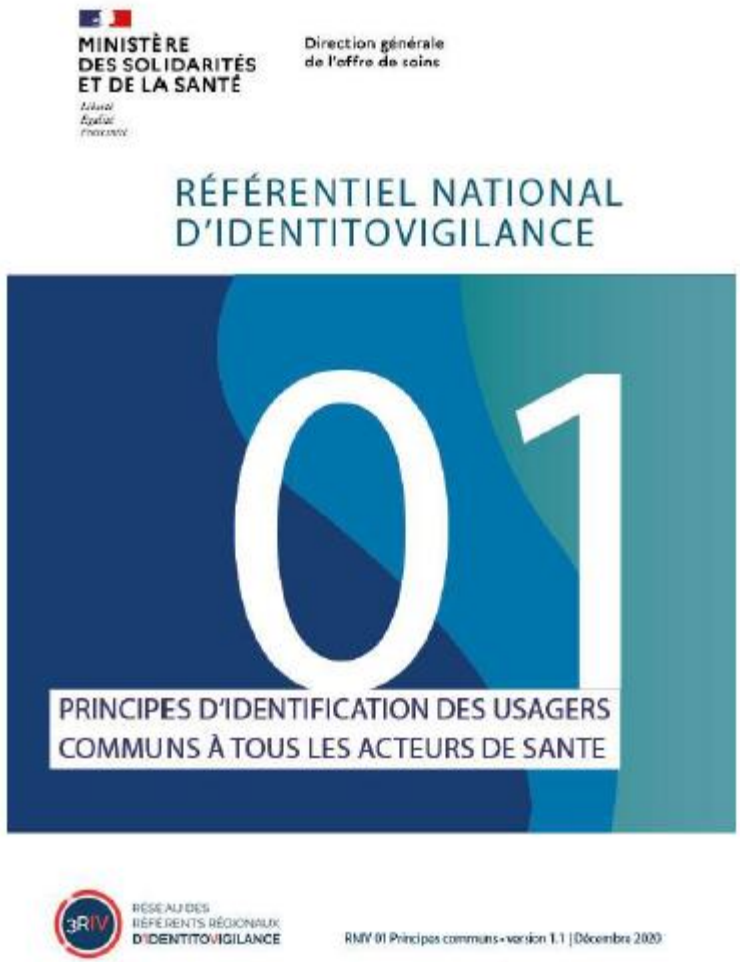


https://solidarites-sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance

Référentiels nationaux actuellement disponibles



Référentiels nationaux actuellement disponibles



- Le RNIV 1 fixe les exigences et recommandations à respecter

- Opposable à tous les acteurs

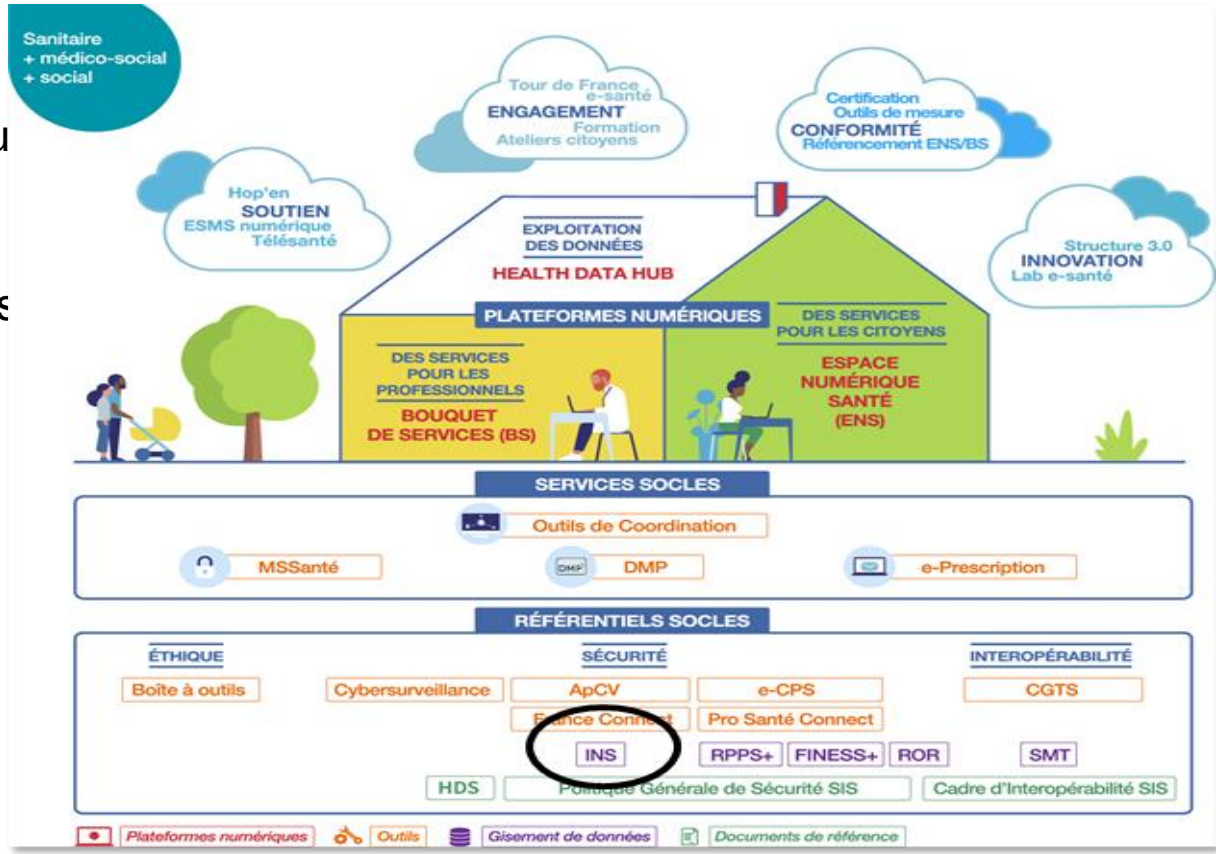
qui traitent des données de santé

- Se substitue aux chartes et référentiels régionaux

RNIV 1 basé sur L'identifiant national de Santé

Contexte

- **L'INS, pierre angulaire du virage numérique**
  - Un des projets socles de la feuille de route nationale du numérique en santé (mesure n° 6)
  - Garantit que l'ensemble des autres projets soient construits sur des fondations solides



POUR RAPPEL

A partir du 1er janvier 2021, toutes les données de santé devront être référencées avec l'INS et les traits d'identité de référence.

https://esante.gouv.fr/MaSante2022/feuille-de-route

L'INS, c'est quoi ?

- **C'est l'identité numérique de référence fournie par le téléservice**

Telle qu'elle est enregistrée sur les bases nationales de référence **RNIPP** (*Répertoire national d'identification des personnes physiques)* et **SNGI** (*Système national de gestion des identifiants)**

- **Appelée « identité INS », elle comprend**

Le *matricule INS* (NIR *numéro d'inscription au RNIPP* ou NIA *numéro identifiant d'attente*)

L'*object identifier* (*OID*) associé au matricule INS, identifiant technique transparent pour les utilisateurs

Les *traits INS* issus des bases nationales de référence

- Nom de naissance
- Prénom(s) de naissance
- Date de naissance
- Sexe
- Code INSEE du lieu de naissance

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

L'INS, pour quels usagers ?

- **Ont une identité INS, les personnes inscrites**
  - Sur le **Répertoire national d'identification des personnes physiques** (RNIPP)
  - Après enregistrement

    Par les services d'état civil (personnes nées en France)

    Ou par l'Assurance maladie (personne étrangère bénéficiant de la couverture sociale française)
- **L'inscription permet d'obtenir**
  - Un numéro d'inscription au **RNIPP** (NIR), au plus tard 8 jours après la naissance

  Ou un numéro identifiant d'attente (NIA) avant l'attribution définitive d'un NIR
- **Le matricule INS**

  Est constitué du NIR ou du NIA

  Est toujours transmis par voie informatique avec son ***OID*** **qui permet de distinguer NIR et NIA**

  Doit être précisé comme « NIR » ou « NIA » quand il est imprimé

L'INS, pour quels usages ?

- **Les usages sont précisés dans le référentiel INS (V1, décembre 2019)**

  – Référencement des données de santé relatives à la prise en charge sanitaire et le suivi médico-social des usagers (y compris les données sociales si elles sont associées)

  – Usage restreint à un nombre limité d'acteurs constituant un *cercle de confiance*

pour ces acteurs, le référencement des données de santé avec l'identité INS est obligatoire si :

- L'identité numérique locale est *qualifiée* (identité INS + vérification par procédure *ad hoc*)
- Il n'existe aucun doute sur l'identité de la personne prise en charge
- La prise en charge n'est pas réalisée dans un cadre réglementaire d'anonymat

L'appel au téléservice

Les 2 opérations du téléservice

1.Récupération de l'identité INS

2.Vérification de l'identité INS

Il est nécessaire de se doter d'une carte CPX nominative pour accéder au téléservice INSi

Comment fonctionne l'opération de récupération de l'identité INS

1. Récupération de l'identité INS

Comment

Lecture automatique de la **carte vitale**

Saisie des traits d'identité:
Nom de naissance
1 des prénoms de naissance
Date de naissance et sexe

Données retournées

- Nom de naissance
- Prénom de naissance (liste)
- Date de naissance
- Sexe
- Lieu de naissance (code INSEE)
- Matricule INS

Comment fonctionne l'opération de vérification de l'identité INS

2. Vérification de l'identité INS

Quel usage ?

Vérification d'une identité INS **transmise par un professionnel**

Comment ?

Envoi de l'INS et des traits d'identité du patient et **retour du service OK ou KO**

Diffusion de l'INS

- **Diffusion de l'INS en interne**

Toutes les applications qui traitent des données de santé doivent à terme référencer ces données de santé avec l'identité INS

- **Diffusion de l'INS vers l'extérieur**

Document publié sur le site de l'ANS :

« Prise en charge de l'identifiant national de santé (INS) dans les standards d'interopérabilité et les volets du CI SIS » a été publiée sur le site de l'ANS »

En pratique au bureau des admissions:

- Vérification de l'identité selon les procédures d'identito-vigilance mises en place au sein de l'établissement

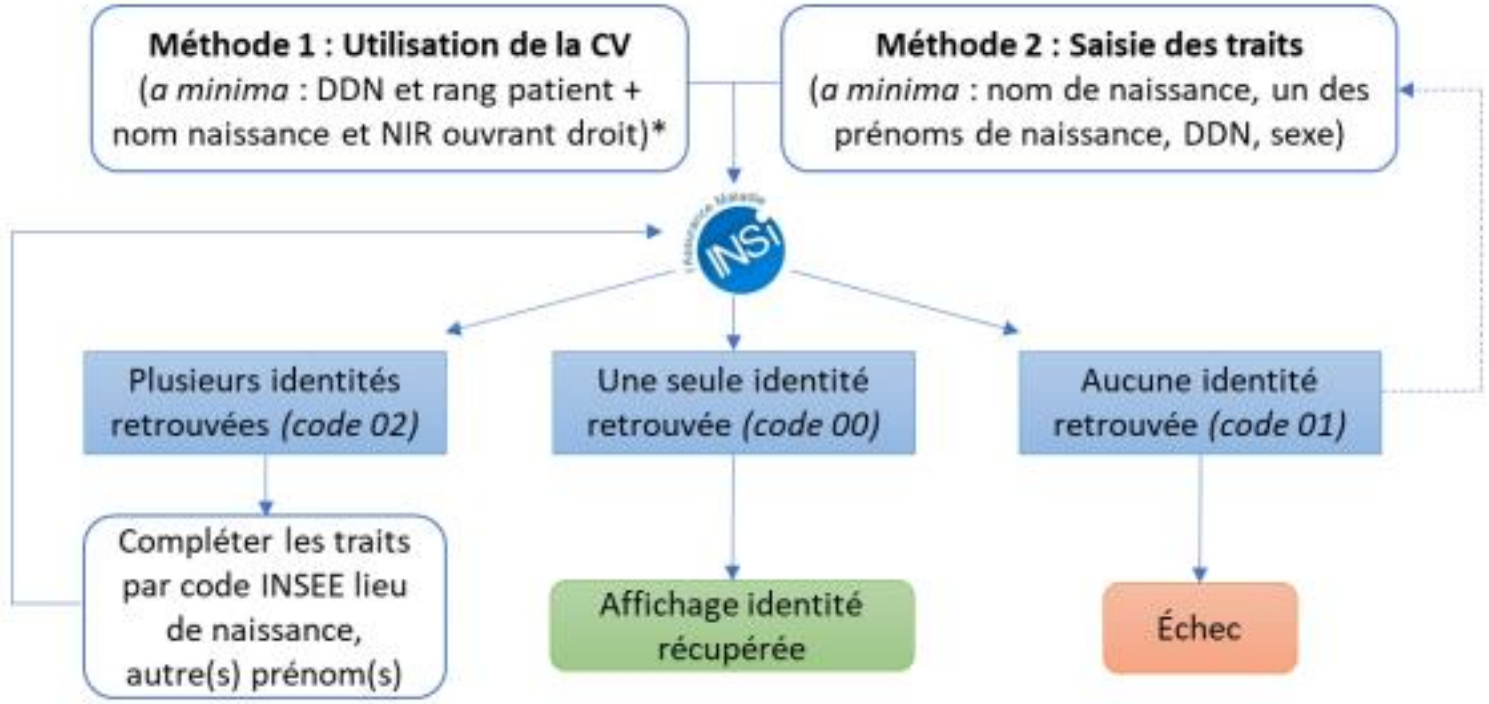
- Utilisation du téléservice INSi pour s'assurer de la conformité avec les bases nationales de référence et « récupérer » l'INS

Exi PP 01 appel au teleservice obligatoire si l'identité n'a jamais été récupérée

- Recherche de l'identité numérique dans le système d'information

Exi SI 01 effectuer la recherche à partir de l'identité INS récupérée par l'INSi, ou à partir de la saisie de la DDN complétée par les 1ers caractères du nom/prénom

Création d'une identité :



Pour obtenir des résultats pertinents(…) limiter le nombre de caractères saisis

Exi PP 06 privilégier interrogation INSi par la carte vitale

Exi SI 06 les informations récupérées font l'objet d'un stockage et d'une traçabilité dans le système d'information local

Les informations INSi:

- Les traits récupérés ramenés par le téléservice sont :

  - Nom de naissance
  - La liste des Prénoms
  - Sexe
  - Date de naissance
  - Lieu de naissance (code commune INSEE)

- Avec des règles syntaxiques qui changent ! :

  - Lettres majuscules non accentuées (A à Z)
  - Espace
  - Caractères spéciaux (apostrophe, tiret, double tiret)

Traits d’identité stricts à vérifier à l’aide d’une pièce d’identité

vs

Traits rapportés par l’INS (RNIV1 annexe IV)

Evaluer la cohérence des traits avant d’accepter l’enregistrement dans le système d’information local (RNIV1 annexe VI)

Exi PP 05 avant toute intégration de l’identité INS dans le système local il est nécessaire de valider la cohérence INSi/ personne physique

Traits stricts vs traits INS, évaluer la cohérence

Nom de naissance

- Enregistré en majuscule
- Trait d'union et apostrophes conservés sur traits INS. A intégrer (RNIV 1)
- Autres caractères remplacés par un espace
- Si étranger sans précision du nom de naissance : enregistrement « aux dires de l'usager » et statut d'identité provisoire

Date de naissance

- *Exi SI 15 Le système d'information doit permettre la traduction d'une ddn en calendrier luni-solaire pour les usagers , au format jj/mm/aaaa*
- S'il manque le jour ou le mois mettre 01
- S'il manque le jour et le mois mettre 31/12

Traits stricts vs traits INS, évaluer la cohérence

INS fait apparaitre tous les Prénom(s) de naissance

- Enregistrés comme apparaissent sur la pièce d'identité
- Les virgules sont transformées en espace

1er prénom de naissance : trait strict attendu

- 1er prénom avant la virgule, comme enregistré sur la pièce d'identité

Traits stricts vs traits INS, évaluer la cohérence

sexe

- M/F/I
- En cas de réassignation sexuelle, enregistrement sur la base du jugement du tribunal administratif faisant apparaitre l'ancienne et la nouvelle identité. Mais validation de l'identité uniquement si présentation d'une pièce d'identité avec la nouvelle identité.

Lieu de naissance

- Code INSEE des communes
- Etrangers : Code INSEE du pays (qui commence par 99)
- Si inconnu : coder 99999

Les traits d'identité complémentaires dans le RNIV 1

Exi SI 05 le système doit permettre la saisie des traits complémentaires Nom utilisé et Prénom utilisé

Nom utilisé

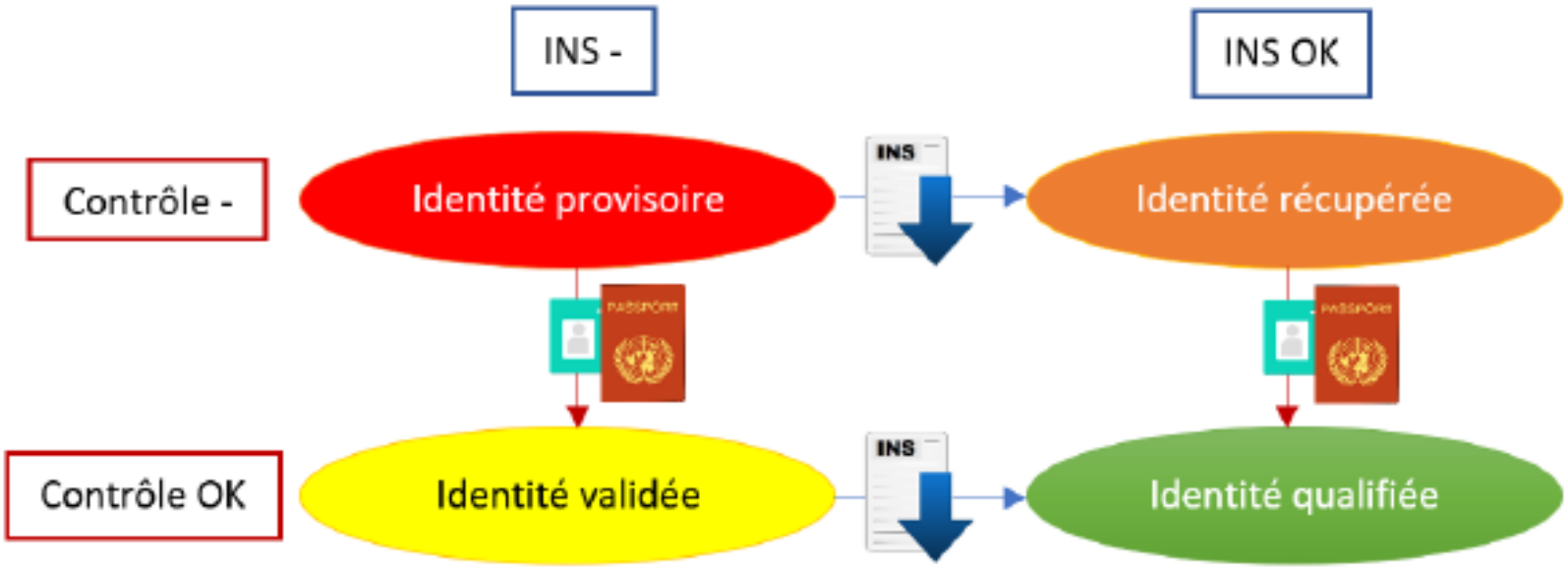
- Obligatoire si différent du nom de naissance.
- Choix de structure de **limiter à nom d'usage** comme mentionné sur pièce d'identité **ou** d'accepter d'enregistrer **tout nom effectivement utilisé par l'usager** (sur sa demande expresse , si trait constant utilisé à chaque venue et si la structure l'autorise)
- Choix de structure de le rendre obligatoire même quand nom utilisé = nom de naissance.

Exi PP17 enregistrement nom utilisé obligatoire si différent nom naissance

Prénom utilisé

- Prénom utilisé par l'usager dans la vie courante
- Choix de structure de limiter à l'enregistrement d'un des prénoms établis à l'état civil (prénom d'usage) ou d'accepter d'enregistrer tout prénom effectivement utilisé par l'usager (sur sa demande expresse , si trait constant utilisé à chaque venue et si la structure l'autorise)
- *Exi PP18 enregistrement prénom utilisé obligatoire si différent 1er prénom naissance*

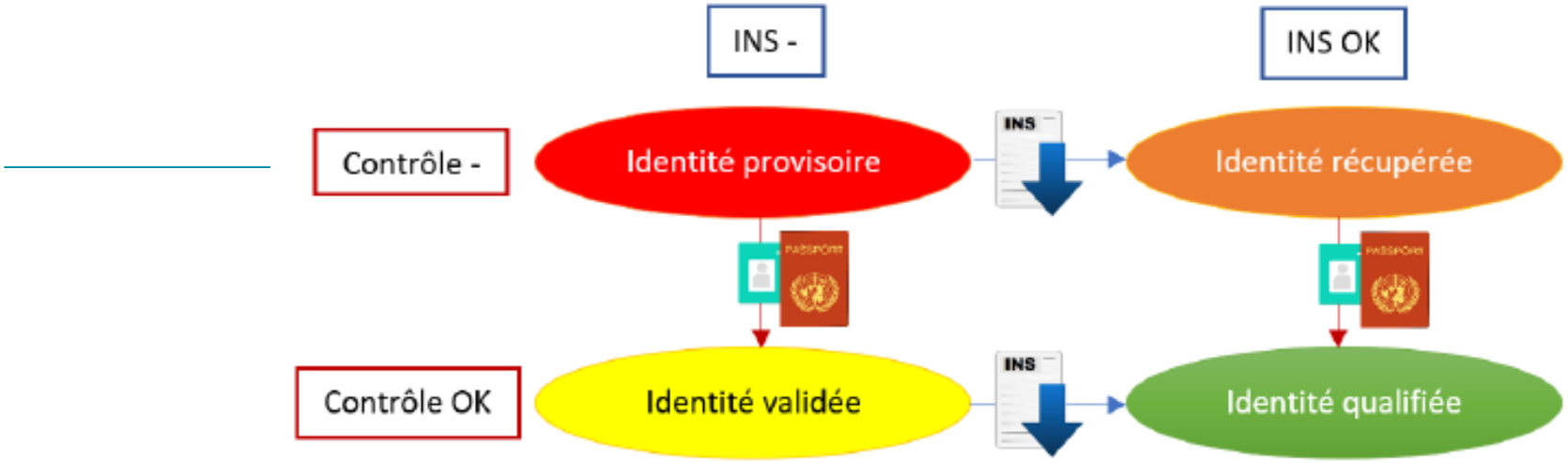
Attribution d’un statut de confiance



Exi SI 07 - Exi PP 07 L’attribution d’un niveau de confiance à toute identité numérique est obligatoire.

Exi PP 08 –Exi PP 09 contrôler la cohérence à la lumière d’un titre de haut niveau de confiance et au regard de la personne physique

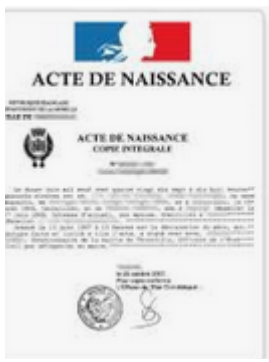
Exi SI 08 Le système d’information doit garantir que seul le statut Identité qualifiée permette le référencement des données de santé échangées avec le matricule INS



- *Exi SI 12 Après attribution du statut « id. récupérée », les traits INS doivent remplacer les traits stricts locaux dans les champs correspondants*

- *Exi PP 11 dès passage au statut « qualifiée » le matricule ET les traits INS doivent être utilisés lors des échanges de données de santé*

Pièces à haut niveau de confiance



Acceptés pour les mineurs si l'identité du parent peut être également vérifiée

- NB : une date de validité dépassée n'empêche pas de « valider » une identité

Tous les autres documents ont une valeur plus faible et ne permettent pas de valider une identité numérique (RNIV 1 p.12)

Si incohérence (RNIV 1 ANNEXE VI)

- S'il y a une erreur de saisie manuelle, une erreur de sélection de dossier avant appel INSi ou de la sélection du bénéficiaire sur la carte vitale utilisée
- Ou si Différence entre titre d'identité et traits INS

→Valider les différences acceptables (code INSEE, présence trait d'union..) et alors les traits INS deviennent ceux à utiliser

Sinon refuser l'identité INS

- Si incohérence sur pièce d'identité : inviter l'usager à la faire corriger à l'état civil
- Si incohérence sur base nationale: inviter l'usager à faire une demande de correction d'état civil à l'INSEE
- Si constaté après avoir récupéré l'INS, déclasser en « identité provisoire », ce qui doit supprimer l'INS associé

Concernant l'AFFICHAGE (RNIV1 annexe VIII)

Exi SI 11 les traits affichés doivent être facilement distingués, sans risque d'équivoque

Exi PP10 Afficher a minima les traits stricts, et si l'identité est qualifiée, l'INS suivi de sa nature (NIR ou NIA), **notamment lors des échanges de données.**

Sans risque de confusion

Sur une étiquette ou une interface homme machine (Exi PP10) :

peut se limiter aux traits stricts (nom naissance, 1er prénom naissance, ddn et sexe)

+ nom et prénom utilisé, et si besoin IPP

Si l'INS est transmis, l'OID n'a pas d'interet mais la nature du trait (NIR ou NIA) permettra au destinataire de faire appel au teleservice !

Si tous les caractères du nom et prénom ne peuvent être affichés, il est nécessaire de le signaler par un astérisque (*) à la fin de la chaine de caractères affichés

NB: Attention à ce que le caractère ne se transforme pas lorsque l'information descend dans un autre logiciel !

Gestion des risques

RNIV 1 évoque les principes généraux:

- Documentation spécifique à l'identitovigilance

  Exi SI 13 référentiel unique d'identités

  Exi PP 12 Cartographie des flux entre applications et type d'interface

  Exi PP 13 droits et habilitations dans charte informatique

  Exi SI 14 traçabilité des modifications

  Fonctionnalité recherche des anomalies

  Exi PP 14 procédure d'alerte si diffusion d'une

  erreur en lien avec l'identité INS

  Opération de vérification des identités qualifiées tous les 3-5 ans

Gestion des risques

RNIV 1 évoque les principes généraux (suite) :

- Cartographie des risques a priori
- *Exi PP 15 politique / Charte locale d'identitovigilance*
- Procédures pour contrôle de cohérence dans les actes importants
- Participation active des usagers
- Système de signalement des erreurs (administratives ou dans les soins)
- Retours d'expérience
- Formation des professionnels
- Vérification cohérence d'affichage entre les différents logiciels

Agence Régionale de Santé Bourgogne-Franche-Comté

e-santé Bourgogne - Franche - Comté

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

Direction générale de l'offre de soins

RÉSEAU DES RÉFÉRENTS RÉGIONAUX D'IDENTITOVIGILANCE

RNIV 02 Identitovigilance en établissements de santé • version 1.1 | Décembre 2020

Le Référentiel National D'IDENTITOVIGILANCE 02

La mise en œuvre de l'identitovigilance dans les établissements de santé

2021

Objet du document

Pérenniser l'implication des ES à lutter contre les erreurs d'identité

Le RNIV 02 :

- Précise les préconisations opposables aux établissements de santé ou aux groupements de structures, publics ou privés
- Complète les règles et recommandations du RNIV 1 notamment en matière de gestion des risques

Formaliser une politique d'identitovigilance échelon local/territorial

Gouvernance et identitovigilance

Adaptation des moyens de pilotage (…) selon les ressources humaines disponibles, selon l'évaluation des risques associés à son activité, selon les populations accueillies et définie dans une charte d'identitovigilance

- Une instance stratégique
- Une instance opérationnelle avec un référent ID
- Une instance consultative

Exi ES 01 instance stratégique et opérationnelle dédiées doivent être mises en place par les établissements

Formaliser une instance stratégique

(Peut être au niveau du GHT)

Missions

- Participe à la définition de la politique et sa communication
- Arrête l'organisation à mettre en œuvre
- Définit les moyens
- Valide le plan d'actions
- Effectue le suivi des actions (indicateurs)
- Décide des actions correctrices

Règlement intérieur, CR de réunion (au moins semestrielle) ou relevé de décision, et plan d'actions

Composition

Désignation en CME

- Le directeur
- Le président de CME
- Le DSI
- Le médecin DIM
- Le responsable des admissions
- Le référent en ID
- Le responsable des SI
- Le responsable QGDR
- Le coordonnateur GDRAS
- Le délégué à la protection des données, + (pharma, hémo, archives…)

Formaliser une instance opérationnelle ou cellule d'identitovigilance (CIV)

Missions

- Participe à la formation des professionnels (plan de formation institutionnel, nouveaux arrivants…)
- Mène des actions auprès des usagers et partenaires externes
- Analyse les risques *à priori* (cartographie)
- Formalise les documents qualité (veille réglementaire)
- REX des EI
- Suit les indicateurs
- Réalise des audits de pratiques

…

Composition

Désignation par le responsable de la structure, sous autorité du référent en ID

- Tous professionnels compétents en ID (médicaux, paramédicaux, administratifs, médico-techniques…)

(Préconisation en ETP annuels à titre indicatif (page 5 du RNIV 02)

Règlement intérieur, CR de réunion ou relevé d'informations/décisions. Fonctionnement quotidien

Nommer le référent en identitovigilance

Exi ES 02 un référent doit être identifié dans tout établissement de santé.

Nommé par la direction (+CME), Fiche de poste, Temps dédié

(peut être au niveau local ET au niveau du GHT)

Ses missions :

- Promouvoir les bonnes pratiques
- Piloter la CIV
- Représenter la structure dans l'instance consultative régionale
- Participer à la gestion des risques
- Alerter le responsable de la structure sur les difficultés rencontrées

L’instance consultative

Pas obligatoire (décision de l’instance stratégique)

Si elle existe :

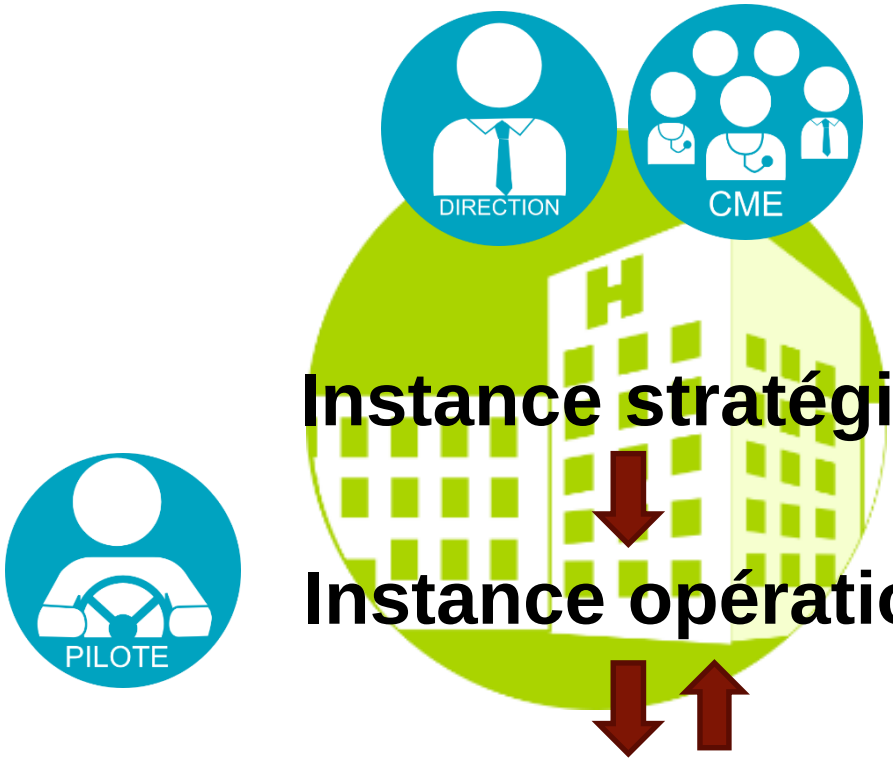
Constituée de représentants des différentes catégories socio professionnelles impliqués dans les questions d’identitovigilance

(peut être mise en place au sein d’un GHT)

Sa mission :

- Donner son avis sur la politique, la formation, les documents qualité, qui lui sont soumis

Schéma récapitulatif de l'organisation locale/territoriale



Gestion documentaire

- Une charte d'identitovigilance
- Des procédures opérationnelles
- Documents opérationnels

➢ Charte d'utilisation du SI de santé

➢ Cartographie des flux applicatifs

➢ Les habilitations (droits d'accès, droits de créations et modification d'identité, droits de rapprochement et de fusion, rôles des référents logiciels)

Formaliser la gestion des risques relative à l'identitovigilance

- **La cartographie des risques *a priori***

Balayer avec un panel représentatif de professionnels, les situations problématiques susceptibles d'être rencontrées dans les différentes activités de la structure , recenser les moyens existants et anticiper des mesures barrières

- **La gestion des évènements indésirables (système interne à la structure) *a posteriori***

Circuit de recueil des évènements indésirables de l'identification primaire et secondaire en interne (voir externe en cas d'évènement grave associé aux soins)

Formaliser la gestion des risques relative à l'identitovigilance (suite)

- **Les retours d'expériences ciblés**

✓ Analyse des facteurs institutionnels, organisationnels, humains

✓ Mise en œuvre d'actions correctrices dans les meilleures délais

✓ Compte-rendu (anonymisé) transmis à l'instance opérationnelle

Sécuriser les démarches d'identification primaire

- **Identification primaire :**

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.

Il est interdit de pratiquer des « validations automatiques » des identités numériques au bout d'un certain délai, sans passer par l'étape obligatoire de contrôle de cohérence des traits de l'identité numérique avec ceux portés sur un dispositif d'identité à haut niveau de confiance

Moyens de sécuriser l'utilisation des identités numériques?

- **Le référentiel d'identité**

Ensemble de composants du SI garantissant la cohérence des données d'identité dans les logiciels métiers

- **La prévention et la gestion des collisions**

Correspond à l'utilisation d'un même identifiant pour au moins 2 personnes physiques différentes.

- Formation des acteurs
- Attention des usagers
- Procédures d'accueil pour éviter une utilisation frauduleuse

Moyens de sécuriser l'utilisation des identités numériques?

- **Propagation des modifications d'identité**
  - Protocole d'interopérabilité

- **Contrôle qualité de la base d'identités numériques**
  - Recherche de doublons

- **Fusions d'identités numériques au sein du domaine d'identification (PR spécifique)**

La fusion des identités numériques ne peut être réalisée que par des professionnels spécialement formés et habilités (et validation médicale si présence de données médicales) + communication aux acteurs et traçabilité de l'opération

Sécuriser l'enregistrement de l'identité numérique locale?

- **Modification d'identité numérique (PR spécifique)**

Habilitation des personnes, communication des acteurs et traçabilité de l'opération

Le rattachement à une nouvelle identité INS ne peut être réalisé que par interrogation du téléservice INSi.

- **Contrôle qualité de la saisie manuelle**

Participation/vérification par l'usager, autre professionnel

- **Repérer les écarts**

➢ opération de vérification tous les 3 à 5 ans préconisée par le référentiel INS

Sécuriser la gestion des identités approchantes?

Concernent :

- Les usagers homonymes vrais, qui partagent plusieurs traits stricts et notamment le nom de naissance, le premier prénom, le sexe, date de naissance ;
- Les autres situations d'identités entre individus dont les traits diffèrent peu (exemple : DUPONT et DUPOND, Jean ANDRE et André JEAN).

➢ PR → mettre en place des garde-fous pour éviter le risque de collision accidentelle des données par erreur de choix de dossier entre 2 identités numériques approchantes dans les opérations administratives et soignantes

➢ Gestion des alertes

Gérer une suspicion d'utilisation frauduleuse d'identité?

Cette substitution frauduleuse, qui relève de la qualification pénale d'escroquerie, est potentiellement dangereuse pour la santé lorsqu'elle entraîne la collision de données entre le fraudeur et un usager déjà enregistré dans la structure.

- Définir les signaux d'alerte (formation)
- Sensibilisation des usagers
- Création d'un dossier provisoire
- Signalement interne de l'évènement indésirable (et externe: alerte CPAM…)

Il est recommandé de réaliser un signalement externe aux autorités compétentes en cas de suspicion d'utilisation frauduleuse de l'identité d'autrui (qui cherche à obtenir indument des prestations sanitaires).

Sécuriser les démarches d'identification secondaire

- **Identification secondaire**

s'assurer systématiquement de la cohérence entre l'identité de l'usager physique et l'identité portée sur la prescription / le document / le dossier / le geste technique qui le concerne(nt).

Plusieurs recommandations peuvent être faites pour améliorer les pratiques dans ce domaine. Il s'agit de vérifier que l'usager bénéficiaire de l'acte est bien celui pour lequel l'acte a été prescrit.

Sécuriser l'identification de l'usager?

- **Identification orale**

Demander de décliner l'identité avec des questions ouvertes

- **Dispositifs d'identification physique (PR)**

Bracelet (avec données informatisées), photographie

Procédure décrivant l'information de l'usager, la préparation, la pose et dépose du bracelet, modalités pratiques d'utilisation…

Il est recommandé d'utiliser un dispositif d'identification physique pour tous les usagers incapables de décliner leur identité.

Sécuriser les documents de PEC ?

- **Identification des informations relatives à l'usager** sur tous les documents

Signaler à l'expéditeur si une anomalie est constatée

- **Contrôle de la cohérence à chaque étape de la prise en charge du patient**, (déclinée ou relevée sur le dispositif d'authentification physique) et celle relevée sur les documents (prescription, pilulier, étiquette, comptes rendus…)

Former les professionnels

Exi ES 04 La formation et la sensibilisation des professionnels à l'identitovigilance doit faire partie des actions du plan de formation annuel des établissements de santé

Sensibiliser les usagers

- **informés au plus tôt des documents qui leur seront demandés** tout au long de leur prise en charge programmée (document d'identité officiel notamment).
  - ✓ Présentez votre pièce officielle d'identité (carte identité, passeport) quel que soit votre interlocuteur : à l'hôpital, en maison de convalescence, au cabinet de radiologie, chez votre médecin traitant...
- **Sollicités pour vérifier ses étiquettes, son bracelet, les documents remis…:**
  - ✓ Vérifiez votre identité et signalez les erreurs, c'est important pour la sécurité de vos soins
- **Invités à décliner son identité autant de fois que demandé et à interroger le soignant en cas de doute sur le traitement, les soins…:**
  - ✓ Une erreur d'identité c'est potentiellement une erreur médicale
  - ✓ Un identifiant unique dans vos soins : l'identité INS (droit d'information pas de droit d'opposition

Pour en savoir plus

- **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

- **Page INS du site de l'ANS**

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

https://solidarites-sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance

- **Page régionale**

https://www.requa.fr/sanitaire/100/cellule-regionale-d-identitovigilance-criv-ars-requa-grades.html?action=afficherP&idA=1&idP=551

https://www.bourgogne-franche-comte.ars.sante.fr/identito-vigilance-en-bourgogne-franche-comte

- **Nous contacter**
  - Armelle Gonzalez Armelle.Gonzalez@esante-bfc.fr
  - Aurelie Agius Aurelie.Agius@esante-bfc.fr
  - Sylvie Boucard sylvie.boucard@requa.fr
  - Juliette Vabre juliette.duchene@requa.fr