FACS OCCITANIE

Fédération des Acteurs de la Coordination en Santé

GUIDE DE BONNES PRATIQUES EN IDENTITOVIGILANCE

AU SEIN DES ACTEURS DE LA COORDINATION EN SANTE

V1-2025

SOMMAIRE

GUIDE DE BONNES PRATIQUES EN IDENTITOVIGILANCE

PREAMBULE

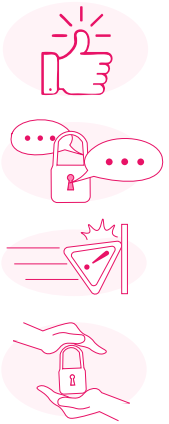
L'identification fiable des usagers est une condition essentielle à la sécurité et à la qualité des parcours de santé. Dans un contexte de coordination croissante entre professionnels, la fiabilité de l'identité constitue un enjeu stratégique, tant pour la continuité des soins que pour la protection des données personnelles.

Les dispositifs de coordination en santé, par leur rôle transversal et leur intervention auprès d'acteurs multiples (professionnels de santé, travailleurs sociaux, établissements, aidants), sont particulièrement exposés aux risques d'erreurs d'identification. Ces erreurs peuvent entraîner des ruptures de parcours, des doublons, des échanges de données erronées ou encore des retards de prise en charge.

Il s'inscrit dans la stratégie nationale autour de l'Identité Nationale de Santé (INS), portée par l'Agence du Numérique en Santé (ANS), et répond aux exigences du RGPD en matière de fiabilité des données personnelles.

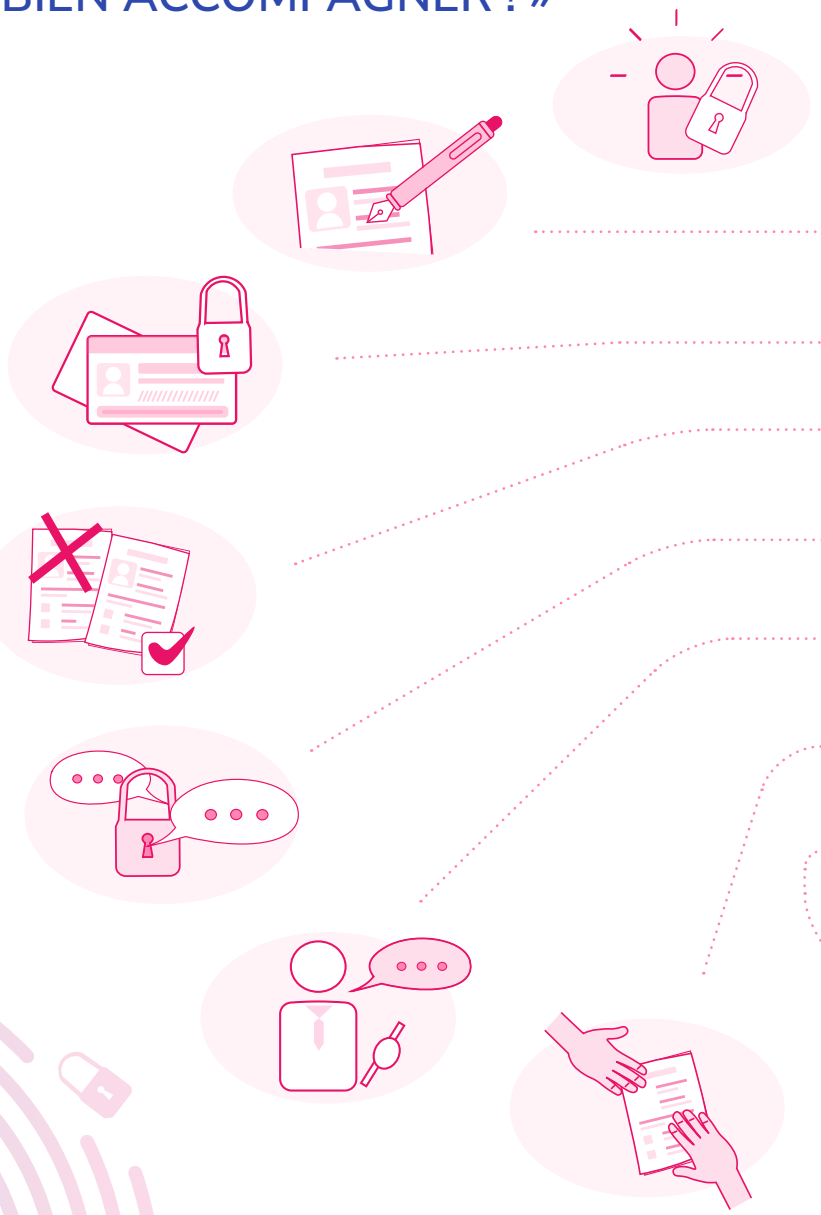
Ce document est destiné à tous les professionnels, qu'ils interviennent en « front office » (accueil, saisie), en coordination, en gestion administrative ou en appui technique. Il a vocation à être partagé, discuté, adapté et enrichi selon les spécificités locales et les retours de terrain.

Ce guide de bonnes pratiques en identitovigilance a été conçu pour accompagner les professionnels dans leur quotidien, en leur fournissant des repères clairs, des conseils concrets et des outils opérationnels pour :



- **Garantir** l'identification correcte des usagers,
- **Sécuriser** les échanges d'informations,
- **Prévenir** les erreurs liées à l'identité,
- **Favoriser** une culture partagée de l'identitovigilance au sein des équipes.

« BIEN IDENTIFIER, C'EST BIEN ACCOMPAGNER ! »



- **Identifier** l'usager de manière fiable
- **Saisir les données** selon l'état civil
- **Utiliser** l'Identité Nationale de Santé (INS)
- **Prévenir** les doublons et collisions
- **Sécuriser** les échanges de données
- **Informer** l'usager avec pédagogie
- **Travailler en lien** avec le référent identitovigilance
- **S'inscrire dans** une dynamique collective

« PAS DE COORDINATION SANS BONNE IDENTIFICATION ! »

C'EST QUOI L'INS ?

L'Identifiant National de Santé (INS) est un identifiant officiel, unique et obligatoire pour chaque usager du système de santé. Il est obligatoire depuis janvier 2021 et **permet de sécuriser l'identification et d'éviter les erreurs dans les parcours de soins et la coordination.**

L'INS ne s'invente pas, elle se récupère, se vérifie, se trace. Il s'agit d'une donnée sensible à utiliser seulement si nécessaire et jamais sur des supports non sécurisés.

A QUOI SERT L'INS ?

- Éviter les erreurs d'identité ou de doublons
- Assurer une coordination sécurisée entre acteurs
- Alimenter le DMP et utiliser MSSanté
- Partager des informations sans confusion

DE QUOI EST COMPOSÉE UNE INS ?

L'INS est composé :

- Un identifiant unique : le NIR (numéro de sécurité sociale) ou un identifiant technique.
- 5 traits d'identité dits "stricts" : nom et prénoms de naissance, sexe, date et lieu de naissance.

Ces 5 traits sont obligatoires pour interroger le téléservice INSi.

CE QU'UN PROFESSIONNEL DOIT FAIRE

- Collecter les 5 traits d'identité stricts
- Demander une pièce d'identité quand c'est possible
- Utiliser un outil compatible INSi
- Transmettre l'INS uniquement via outils sécurisés (MSSanté, plateforme certifiée HDS)
- Documenter le niveau de qualification dans le dossier patient, outil de coordination

TÉLÉSERVICE INSI : À QUOI ÇA SERT ?

Il permet de récupérer l'INS officielle d'un usager à partir des 5 traits d'identité. C'est l'outil clé pour qualifier l'identité des usagers en toute sécurité.

Il est intégré dans certains logiciels compatibles (ex : SPICO DOSSIER) et est accessible avec une CPS ou e-CPS.

L'INS "QUALIFIÉE" : COMMENT ?

Une INS est qualifiée si :
1.Elle est récupérée via le téléservice INSi
2.L'identité a été vérifiée à l'aide d'une pièce d'identité officielle

Il s'agit du niveau exigé pour l'intégrer dans un document de santé (courrier, transmission, etc.). L'INS récupérée doit être intégrée et conservée dans le dossier avec son niveau de qualification.

POUR EN SAVOIR +

1 - Identitovigilance : Définition et risques
2 - Identitovigilance : Périmètre et termes utilisés
01 - INS : Qu'est-ce que l'INS ?
02 - INS : Qu'est-ce que le téléservice INSi

***Cliquez** sur les liens*
pour accéder aux courtes vidéos réalisées par esanté Occitanie sur le sujet

II. Qu'est-ce que l'identitovigilance ?

L'identitovigilance est l'ensemble des mesures et des bonnes pratiques mises en place pour garantir que chaque usager est identifié de manière fiable, unique et sécurisée, tout au long de son parcours.

Elle permet d'éviter les erreurs liées à une mauvaise identification (confusion entre deux personnes, doublons, identité erronée), qui peuvent entraîner des conséquences graves sur l'accompagnement, la coordination et la confidentialité des données.

Au sein de votre structure, l'identitovigilance est essentielle pour assurer :

- Une communication claire entre les professionnels,
- Une coordination efficace des parcours,
- La protection des données personnelles des usagers.

III. Cadre réglementaire et responsabilités

3.1. CADRE RÉGLEMENTAIRE

L'identitovigilance s'appuie sur plusieurs textes législatifs et réglementaires, qui définissent les obligations en matière d'identification des usagers :

LES PRINCIPAUX TEXTES DE RÉFÉRENCE SONT :

- *Règlement général sur la protection des données (RGPD) – UE 2016/679*

→ Oblige les structures à garantir la sécurité, l'exactitude, la transparence et la finalité des données personnelles collectées.

- *Code de la santé publique, articles L1110-4, L1111-8, R1111-8*

→ Imposent la sécurisation des données de santé et la confidentialité dans le cadre du partage d'informations.

- *Arrêté du 27 mai 2021 relatif à l'Identifiant National de Santé (INS)*

→ Rend obligatoire l'utilisation de l'INS comme identifiant unique dans tout échange de données de santé.

- *Recommandations de la CNIL*

→ Encadrent le recueil, le traitement et la conservation des données d'identité.

III. Cadre réglementaire et responsabilités

3.2. RESPONSABILITÉS

En tant qu'acteur central dans la coordination en santé, les dispositifs ont une double responsabilité : garantir la fiabilité des données d'identité et protéger les droits des usagers.

RESPONSABILITÉS OPÉRATIONNELLES

- Identifier correctement chaque usager à partir d'un justificatif officiel (identité de référence).
- Qualifier l'INS de l'usager pour les échanges avec les partenaires du secteur santé/social.
- Vérifier, sécuriser et mettre à jour les données dans les outils de coordination.
- Documenter les anomalies et les signaler au référent identitovigilance.
- Sensibiliser et former les professionnels internes à ces enjeux.

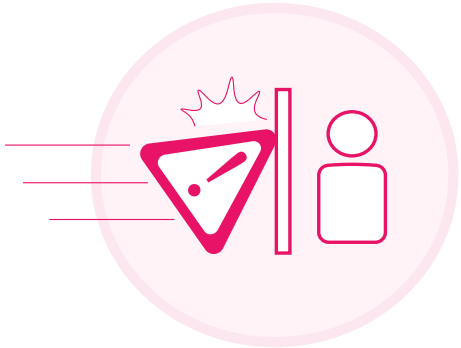
RESPONSABILITÉS JURIDIQUES ET ÉTHIQUES

- Respecter le RGPD : les données personnellesdoivent être licites, exactes, pertinentes, limitées et sécurisées.
- Informer l'usager de ses droits (accès, rectification, opposition).
- Tenir un registre des traitements (obligation pour les structures traitant des données sensibles).
- Assurer une traçabilité des vérifications d'identité et des accès aux données.
- Protéger les personnes en situation de vulnérabilité, en évitant toute discrimination liée à leur statut administratif.

IV. Bonnes pratiques en identitovigilance

Les bonnes pratiques en identitovigilance sont l'ensemble des actions, réflexes et procédures à mettre en œuvre pour garantir l'identification correcte, fiable et sécurisée des usagers dans tous les échanges d'informations. Elles permettent de prévenir les erreurs d'identité, les doublons, les confusions entre personnes, et de protéger les données personnelles et de santé.

Ces bonnes pratiques sont indispensables pour assurer une coordination efficace et respectueuse des droits des usagers, notamment les plus vulnérables.



4

4.1. IDENTIFICATION ET VÉRIFICATION DE L'USAGER

- Demander une pièce d'identité officielle[1]
- Respecter strictement les données d'état civil (orthographe, prénoms, etc.)[2]
- Ne pas qualifier une identité sans justificatif[3]

4.2. GESTION DES DOSSIERS

- Rechercher systématiquement les doublons
- Mettre à jour régulièrement les données
- Utiliser le téléservice INSi pour récupérer l'INS[4]

4.3. SÉCURITÉ DES ÉCHANGES ET TRAÇABILITÉ[5]

- Utiliser des canaux sécurisés (mail professionnel, plateformes sécurisées)
- Supprimer les données sensibles après traitement
- Conserver et archiver les données conformément à la réglementation

V. Processus en cas d'anomalie ou de doute

5

Une anomalie d'identité désigne toute situation où l'identité d'un usager paraît incomplète, incohérente, incertaine ou potentiellement erronée.

Exemples :

- Deux dossiers pour la même personne avec des identifiants différents (doublon),
- Disparité entre les données déclarées et les pièces présentées,
- Absence de justificatif officiel,
- Données incompatibles avec l'INS ou rejet du téléservice INSi.

L'objectif de cette étape est de garantir une prise en charge sécurisée de l'usager malgré le doute, limiter les erreurs, et rétablir une identité fiable, en respectant la réglementation (RGPD, sécurité des soins, confidentialité).

5.1. IDENTIFIER LES ANOMALIES

- Pièces d'identité suspectes ou falsifiées
- Incohérences dans les données (dates, noms, prénoms)
- Présence de doublons[6]

5.2. ACTIONS À MENER

- Ne pas enregistrer l'identité douteuse
- Documenter l'anomalie dans une fiche de signalement[7]
- Informer le référent identitovigilance
- Suivre et analyser les cas récurrents

5.3. BONNES PRATIQUES

- Ne jamais supprimer ou modifier un dossier sans traçabilité.
- Toujours utiliser l'identité **qualifiée** avant tout échange de données sensibles.
- Sensibiliser les professionnels à **ne pas "deviner" ou "corriger" une identité** de leur propre chef.
- Conserver les données sensibles (y compris les anomalies) dans des espaces sécurisés et restreints.

VI. Information et droits des usagers[8]

Tout usager a le droit d'être informé de manière claire, accessible et loyale sur la collecte, l'utilisation et la protection de ses données d'identité (notamment en lien avec l'utilisation de l'INS – Identifiant National de Santé). Ce droit est garanti par le RGPD (Règlement général sur la protection des données) et par le Code de la santé publique, qui imposent transparence, loyauté et respect de la vie privée.

6.1. INFORMER L'USAGER

L'information des usagers est une obligation légale et éthique, fondée sur la transparence, le respect et la protection des personnes.

Les informations à transmettre à l'usager sont les suivantes :

- L'identité du responsable de traitement « Vos données sont traitées par [Nom de la structure], en tant que responsable de traitement. »
- La finalité du recueil des données « Nous collectons votre identité pour garantir un accompagnement sécurisé et éviter toute confusion. »
- La base légale « Ce traitement est fondé sur l'intérêt public, la coordination du parcours de santé et la conformité réglementaire (INS, RGPD). »
- Les destinataires des données « Vos informations peuvent être partagées avec les professionnels impliqués dans votre suivi, dans le respect du secret professionnel. »
- La durée de conservation « Vos données sont conservées pendant [X années], selon la réglementation en vigueur. »
- Les modalités d'exercice des droits « Pour exercer vos droits, vous pouvez contacter notre référent RGPD ou délégué à la protection des données à [email/contact]. »
- **Les droits de la personne**

« Conformément au Règlement Général sur la Protection des Données (RGPD), vous disposez des droits suivants sur vos données personnelles :

- Droit d'accès : vous pouvez obtenir des informations sur les données vous concernant détenues par [Nom de la structure].
- Droit de rectification : vous pouvez demander la correction de données inexactes ou incomplètes.
- Droit d'effacement : vous pouvez demander la suppression de vos données dans certaines conditions (hors obligation légale de conservation).
- Droit à la limitation du traitement : vous pouvez demander la suspension temporaire du traitement de vos données.
- Droit d'opposition : vous pouvez vous opposer à certains traitements, notamment ceux fondés sur l'intérêt public, sauf motif légitime impérieux.
- Droit à la portabilité : si applicable, vous pouvez demander la transmission de vos données à un tiers ou à vous-même.
- Droit de porter réclamation à la CNIL. »

En pratique

- Remettre une fiche d'information claire.
- Intégrer une clause d'information RGPD dans les documents d'accueil.
- Prévoir un référent RGPD et/ou identitovigilance pour traiter les demandes des usagers[9].
- Traiter toute demande d'accès ou de rectification dans un délai d'un mois.
- Conserver la preuve de l'information donnée à l'usager (accusé de réception, mention signée, etc.).

6.2. SITUATION SPÉCIFIQUE

Dans certaines situations, notamment de précarité ou de vulnérabilité ou encore lors de visite à domicile, l'identification fiable des usagers peut s'avérer complexe. Le rôle du dispositif est alors de s'adapter à la situation pour respecter la dignité des personnes, sécuriser leur parcours et rester conforme au cadre réglementaire (RGPD, INS, droits fondamentaux).

EN CAS D'ABSENCE DE PIÈCE D'IDENTITÉ

→ Permettre la prise en charge malgré l'absence de justificatif, tout en posant un cadre temporaire sécurisé.

Bonnes pratiques

- Ne pas refuser l'accompagnement : proposer une solution transitoire.
- Recueillir une attestation sur l'honneur de l'usager mentionnant ses nom, prénom, sexe, date et lieu de naissance.
- Solliciter un tiers de confiance (travailleur social, structure référente, aidant familial) pour appuyer cette déclaration.
- Documenter la situation : indiquer dans le dossier que l'identité est en attente de qualification.

SENSIBILISATION AUX ENJEUX DE L'IDENTIFICATION FIABLE AUPRÈS DES USAGERS

→ Permettre à l'usager de comprendre pourquoi son identité doit être vérifiée et protégée.

Messages à faire passer

- Une identité exacte permet d'éviter les erreurs, les confusions ou les ruptures dans les soins.
- Elle garantit la coordination sécurisée entre les professionnels de santé, du médico-social et du social.
- Elle permet d'accéder aux droits sociaux, médicaux et numériques (DMP, carte Vitale, messagerie sécurisée…).
- Vos données sont confidentielles et protégées : elles ne sont ni partagées à des fins commerciales ni transmises sans nécessité.

Par quels moyens ?

- Fiche simple à remettre : « Pourquoi vous demande-t-on vos papiers ? »
- Affichage dans les lieux d'accueil
- Dialogue bienveillant lors du premier entretien

VII. Organisation interne et formation

7.1. LES RÔLES ET RESPONSABILITÉS AU SEIN DES STRUCTURES DE COORDINATION EN SANTÉ

L'identitovigilance nécessite une organisation structurée et claire. Chaque professionnel, selon son rôle, doit contribuer à la fiabilité de l'identification des usagers.

RÔLES	RESPONSABILITÉS
RÉFÉRENT IDENTITOVIGILANCE	Supervise la mise en œuvre des bonnes pratiques, analyse les signalements, suit les anomalies, forme et conseille les équipes.
COORDINATEURS / RÉFÉRENTS DE PARCOURS / PROFESSIONNELS DE SANTÉ	Recueillent l'identité, vérifient les justificatifs, alertent en cas de doute, appliquent les procédures de signalement.
PROFESSIONNELS ADMINISTRATIFS	Saisissent les données d'identité dans les systèmes d'information, assurent la traçabilité, gèrent la confidentialité.
DIRECTION / RESPONSABLE QUALITÉ	Intègre l'identitovigilance dans le management de la qualité, assure le pilotage, et veille à la conformité RGPD.

7.2. OUTILS À METTRE EN PLACE

- Procédures internes (recueil, vérification, signalement).
- Registre des anomalies d'identité.
- Modèles de fiches et d'attestations.
- Accès sécurisé aux données d'identité.
- Tableau de bord ou indicateurs qualité.

7.3. FORMATION DES PROFESSIONNELS

Pour garantir une pratique fiable et homogène de l'identitovigilance, la formation régulière des professionnels est indispensable.

- Formation initiale et continue.
- Sensibilisation aux risques et enjeux.
- Exercices pratiques et retours d'expérience.

VIII. Annexes

- Annexe 1 - Glossaire : Définitions clés
- Annexe 2 - Bibliographie : Textes réglementaires et recommandations
- Annexe 3 - Contacts utiles : Référents régionaux, autorités de contrôle
- Annexe 4 - Modèles de documents
  - 4.1 Procédure interne
  - 4.2 Fiches bonnes pratiques
  - 4.3 Fiche de signalement d'anomalie
  - 4.4 Checklist d'identitovigilance
  - 4.5 Fiche d'information usager

Annexe 1.1 - Glossaire

• IDENTITÉ USAGER
Ensemble des données officielles permettant d'identifier une personne : nom, prénoms, date et lieu de naissance, sexe.

• IDENTITOVIGILANCE
Démarche visant à assurer la qualité, la sécurité et la fiabilité des données d'identité des usagers pour éviter erreurs, doublons, ou confusions.

• INS (IDENTITÉ NATIONALE DE SANTÉ)
Identifiant unique attribué à chaque personne pour faciliter la coordination et la sécurisation des données de santé.

• RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES)
Règlement européen garantissant la protection des données personnelles et la vie privée des citoyens.

• DONNÉES PERSONNELLES
Toute information se rapportant à une personne physique identifiée ou identifiable.

• DOUBLON
Existence de plusieurs dossiers ou identifiants pour une même personne dans un système d'information.

• QUALIFICATION DE L'INS
Processus d'attribution d'un identifiant INS validé par la vérification d'une pièce justificative officielle.

• RÉFÉRENT IDENTITOVIGILANCE
Personne désignée pour coordonner et superviser les actions relatives à l'identitovigilance au sein d'un établissement ou d'un réseau.

• TÉLÉSERVICE INSI
Service en ligne permettant la consultation et la récupération de l'INS à partir des données d'état civil validées.

• FICHE DE SIGNALEMENT D'ANOMALIE
Document permettant de consigner toute observation ou problème lié à l'identité d'un usager.

Annexe 1.2 - Glossaire des références

(1) Une pièce d'identité est le seul moyen fiable d'assurer la correspondance exacte entre l'usager et ses données. Cela garantit que l'identité enregistrée est conforme à l'état civil. (RGPD art. 5-1d : « Les données doivent être exactes et tenues à jour. » ; Instruction DGOS/ATIH/ ANS sur l'INS : la pièce d'identité est obligatoire pour qualifier une INS.

(2) Respecter l'ordre et l'orthographe des prénoms et noms permet d'éviter les doublons, erreurs ou non-Matching avec les systèmes de santé (DMP, logiciels métiers, etc.). (RGPD art. 5-1a : « Les données sont traitées de manière licite, loyale et transparente. » ; Arrêté du 27 mai 2021 : définit l'identité INS et ses composantes exactes.

(3) Qualifier une INS sans document peut conduire à attribuer une identité à la mauvaise personne. Ce type d'erreur peut avoir des conséquences graves pour l'usager (données erronées, mauvais traitement, etc.). (Risque de violation des droits de la personne (RGPD art. 5-1d & art. 15 à 22) ; INS qualifiée = identité vérifiée sur pièce justificative conforme).

(4) Le téléservice INSi permet de récupérer de manière sécurisée une identité de référence unique. Cela est essentiel pour l'interopérabilité et la coordination entre professionnels. (Obligation légale depuis le 1er janvier 2021 (Instruction ministérielle) ; RGPD art. 32 « obligation de garantir la sécurité et l'intégrité des données personnelles. »

(5) Les données d'identité sont des données personnelles sensibles, au sens du RGPD. Elles ne doivent pas être diffusées de manière non sécurisée. (RGPD art. 32 : mise en œuvre de mesures techniques et organisationnelles ; CNIL : les adresses personnelles, le cloud non professionnel, et les messageries instantanées non sécurisées sont interdits pour les données de santé).

(6) Créer plusieurs dossiers pour la même personne ou enregistrer des données dans le mauvais dossier fausse la coordination, les statistiques, et peut provoquer des erreurs de prise en charge. (RGPD art. 5-1d : exactitude des données ; Règles métiers SI santé : chaque usager doit avoir un seul identifiant INS unique).

(7) Documenter les incertitudes permet de revenir sur la situation, d'éviter la propagation d'erreurs, et de démontrer une gestion responsable des données en cas d'audit. (RGPD art. 30 : obligation de tenir un registre des traitements ; Art. 32 : documentation des actions de sécurisation).

(8) Le RGPD impose une information claire et accessible à la personne concernée sur le traitement de ses données. (RGPD art. 13 et 14 : droit à l'information).

(9) L'identitovigilance est une démarche collective. Avoir un référent permet de structurer les pratiques, de traiter les anomalies, et de former les professionnels. (Recommandations de l'ANS et de la HAS sur l'identitovigilance ; RGPD art. 24 : le responsable du traitement doit démontrer sa conformité.

Annexe 2 - Bibliographie

- **RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL (RGPD) –** Protection des données à caractère personnel, mai 2016.
- **ARRÊTÉ DU 27 MAI 2021** relatif aux caractéristiques et aux modalités d'attribution de l'Identité Nationale de Santé (INS).
- **INSTRUCTION DGOS/ATIH/ANS** sur la mise en œuvre de l'INS dans les établissements de santé et structures médico-sociales, 2020.
- **RECOMMANDATIONS DE LA CNIL** relatives à la protection des données de santé et à la sécurité des échanges, 2022.
- **HAUTE AUTORITÉ DE SANTÉ (HAS) –** Guide méthodologique pour la gestion de l'identitovigilance, 2019.
- **AGENCE DU NUMÉRIQUE EN SANTÉ (ANS) –** Ressources et bonnes pratiques pour l'utilisation de l'INS, 2021.
- **MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ –** Circulaire sur la qualité de l'identification des patients dans le cadre des parcours de santé, 2020.
- **AGENCE NATIONALE DE SÉCURITÉ DU MÉDICAMENT ET DES PRODUITS DE SANTÉ (ANSM) –** Guide pratique sur la sécurité des données patient, 2021.

Annexe 3 - Fiche Contacts Utiles

1. AGENCE DU NUMÉRIQUE EN SANTÉ (ANS)

→ Site web : https://esante.gouv.fr
→ Téléphone : 01 55 93 35 00
→ Email : contact@esante.gouv.fr
→ Services : Support INSi, sécurité des données, ressources d'identitovigilance.

2.COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL)

→ Site web : https ://www.cnil.fr
→ Téléphone : 01 53 73 22 22
→ Email : contact@cnil.fr
→ Services : Réglementation RGPD, accompagnement, signalement des violations.

3.AGENCE RÉGIONALE DE SANTÉ OCCITANIE (ARS OCCITANIE)

→ Site web : https://www.occitanie.ars.sante.fr
→ Téléphone : 04 67 73 58 00
→ Email : ars-occitanie@ars.sante.fr
→ Services : Coordination régionale, référents santé, pilotage des dispositifs DAC.

4.MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

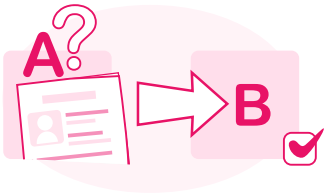
→ Site web : https://solidarites-sante.gouv.fr
→ Téléphone : 01 40 56 60 00
→ Email : dgs-contact@solidarites-sante.gouv.fr
→ Services : Politique nationale santé, recommandations réglementaires.

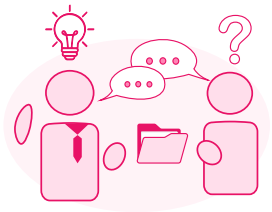
5. SUPPORT TECHNIQUE SI / INSI

→ Service informatique de la structure [A compléter]
→ Hotline INSi régionale : 0 800 123 456 (à vérifier localement)
→ Email support INSi : supportinsi@esante.gou

Annexe 4.1 - procédure interne d'identitovigilance

→ Garantir une identification fiable et conforme des usagers, tout au long de leur accompagnement, en conformité avec le RGPD et les référentiels de l'Identité Nationale de Santé (INS) tout en respectant la dignité et la situation de chacun.





LES PRINCIPES CLÉS

- Respecter la confidentialité et la sécurité des données collectées.
- Informer clairement les usagers des raisons et finalités de la demande de justificatif.
- Proposer une alternative adaptée en cas d'absence ou d'impossibilité de présenter un document officiel.
- Documenter toute anomalie ou absence de justificatif avec traçabilité.
- Assurer un accompagnement pour la régularisation administrative.

Annexe 4.1 - procédure interne d'identitovigilance

1. ACCUEIL / PREMIER CONTACT AVEC L'USAGER

Le professionnel informe l'usager et explique l'importance de la vérification d'identité dans un langage clair et rassurant.

Après avoir présenté la liste des justificatifs acceptés, il demande une pièce d'identité officielle (Carte nationale d'identité, Passeport, Carte de séjour ou titre de séjour en cours de validité).

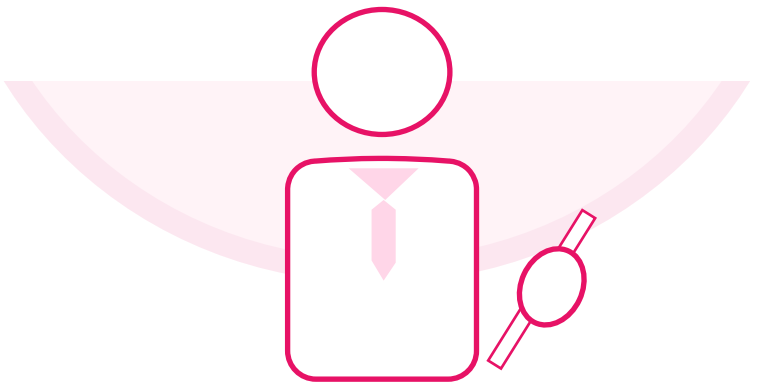
Il réalise une copie ou scanne le justificatif en respectant les règles de protection des données et recueille les informations d'état civil exactes :

- Nom de naissance
- Tous les prénoms dans l'ordre
- Date et lieu de naissance
- Sexe

En l'absence de justificatif, l'identité est déclarée et mentionnée comme telle dans le dossier.

Le professionnel peut alors

- Proposer une attestation sur l'honneur.
- Recueillir, si possible, une attestation d'un tiers de confiance.
- Documenter cette situation dans le dossier usager.
- Proposer un accompagnement pour la régularisation.



Annexe 4.1 - procédure interne d'identitovigilance

2. CRÉATION OU MISE À JOUR DU DOSSIER DANS L'OUTIL MÉTIER OU DE COORDINATION

- Vérification préalable de l'existence d'un dossier pour éviter tout doublon.
- Saisie des données strictement selon l'état civil.
- Récupération de l'INS via INSi :
- Qualification uniquement si une pièce d'identité conforme est fournie.
- En cas d'échec de récupération ou doute : ne pas forcer l'identification.

3. GESTION DES DONNÉES

- Conservation des justificatifs dans un espace sécurisé.
- Restriction de l'accès aux données aux professionnels habilités.
- Suppression ou anonymisation des copies en fin de traitement conformément à la politique de conservation.

4. ÉCHANGES D'INFORMATIONS

- Transmission des données d'identité uniquement via des canaux sécurisés (adresse professionnelle, plateforme sécurisée).
- Suppression des mails contenant des données après traitement.
- Ne jamais transmettre de données identifiantes via des messageries personnelles ou non professionnelles.

5. GESTION DES ANOMALIES OU DOUTES

- Ne pas enregistrer ou poursuivre l'usage d'une identité douteuse.
- Signaler au référent identitovigilance via le formulaire interne.
- Documentation obligatoire dans le dossier (note ou alerte).

6. INFORMATION DE L'USAGER

Information orale (ou via flyer) sur :

- L'utilisation de ses données d'identité
- La finalité de l'INS
- La protection de ses données personnelles (conformément au RGPD)

7. SUIVI ET AMÉLIORATION CONTINUE

Le référent identitovigilance assure :

- L'analyse des signalements
- La mise à jour de la procédure
- La formation continue des professionnels aux enjeux, à la réglementation et à la communication avec les usagers.

Annexe 4.2.1 - Fiche bonnes pratiques

Utiliser le téléservice INSi dans l'outil de coordination

→ Qualifier l'identité d'un usager et fiabiliser les échanges.

1. PRÉPARER LES 5 TRAITS D'IDENTITÉ

Saisir les 5 traits stricts dans la fiche usager : Nom et prénom de naissance, sexe, date et lieu de naissance. Ces informations sont indispensables pour interroger INSi.

2. S'AUTHENTIFIER

Se connecter avec e-CPS ou carte CPS (selon la configuration de votre poste).
Accès sécurisé obligatoire pour utiliser le téléservice.

3. LANCER L'INTERROGATION INSI

Cliquer sur "Appeler le téléservice INSi", SPICO interroge l'Assurance Maladie et récupère automatiquement :

- L'Identifiant INS
- Les traits d'identité officiels
- Le type d'identifiant (NIR ou identifiant technique)

4. VÉRIFIER L'IDENTITÉ

Demander et contrôler un document d'identité officiel (CNI, passeport, titre de séjour, etc.). Vérifier que les données récupérées correspondent bien au justificatif.

5. QUALIFIER L'INS

Si l'identité est bien vérifiée et récupérée via le téléservice alors l'INS est qualifiée.

Noter dans le dossier :

- La date de qualification
- Le type de pièce d'identité vérifiée
- L'auteur de la vérification (nom, prénom, fonction)

À retenir

- Pas de document de santé sans INS qualifiée
- L'INS se récupère via le téléservice et se valide avec une pièce d'identité officielle et se trace systématiquement dans l'outil de coordination.

Annexe 4.2.2 - Fiche bonnes pratiques identitovigilance sans document d'identité fiable

→ Assurer une identification aussi fiable que possible même en l'absence de pièce d'identité officielle, tout en limitant les risques d'erreurs.

1. RECUEILLIR LES DONNÉES DÉCLARÉES PAR LE PROFESSIONNEL REQUÉRANT OU L'USAGER

- Nom de naissance
- Tous les prénoms dans l'ordre
- Date de naissance complète
- Lieu de naissance (commune et pays)
- Sexe

Préciser dans le dossier que l'identité est déclarative non vérifiée.

2. CRÉER UNE IDENTITÉ TEMPORAIRE OU NON QUALIFIÉE

Si le système le permet, créer un profil provisoire
Mentionner :

→ Identité déclarée – justificatif non fourni
→ À fiabiliser ultérieurement

⚠ Ne pas qualifier l'INS sans pièce officielle.

3. VÉRIFIER VIA DES PARTENAIRES

Avec l'accord de l'usager, contacter, si nécessaire :

- Médecin traitant
- Travailleur social
- Établissement ou structure déjà en lien
- Aidant ou représentant légal

Toujours respecter le secret professionnel et noter les sources consultées.

4. ENCOURAGER L'USAGER À FOURNIR UNE PIÈCE D'IDENTITÉ

- Expliquer les risques d'erreur d'identification
- Aider à engager des démarches si besoin (via service social, mairie, etc.)
- Planifier un rappel ou un suivi pour obtenir le document ultérieurement

Annexe 4.2.2 - Fiche bonnes pratiques identitovigilance sans document d'identité fiable

5. TRACER ET INFORMER

Dans le dossier, ajouter une note ou identifier le statut d'identité si l'outil le permet :

- **4 STATUTS D'IDENTITÉ**

STATUTS	DÉFINITION	FABILITÉ	CAS D'USAGE
1.IDENTITÉ PROVISOIRE	Identité saisie sans vérification de pièce d'identité et sans recours au téléservice INSi	**FAIBLE**	Orientation urgente (via appel de l'usager, proche ou partenaire) sans pièce d'identité. Signalement d'un cas par un professionnel partenaire sans document officiel.
2. IDENTITÉ VALIDE	Identité saisie et vérifiée à l'aide d'une pièce d'identité officielle, mais sans appel au téléservice INSi	**MOYENNE**	Rencontre physique avec l'usager avec pièce d'identité, mais pas d'accès immédiat au téléservice INSi.
3.IDENTITÉ RÉCUPÉRÉE	dentité récupérée via le téléservice INSi, sans vérification de pièce d'identité	**BONNE**	L'usager fournit sa carte Vitale ou la structure utilise le téléservice INSi à partir de données déclaratives (nom, date de naissance, etc.), sans vérifier la pièce d'identité.
4. IDENTITÉ QUALIFIÉE	Identité récupérée via INSi ET vérifiée par une pièce d'identité (procédure complète INS)	**TRÈS HAUTE**	Coordination formalisée avec documents de santé, transmissions MSSanté, DMP, etc. Situation nécessitant l'envoi de documents ou d'informations avec l'INS conforme Suivi pérenne ou échanges structurés avec les professionnels de santé

- Note à ajouter si absence de statut d'identité : "Identité déclarée. Vérification documentaire à faire dès que possible."
- Signaler les situations récurrentes ou à risque au référent identitovigilance.

Annexe 4.2.3 - Fiche bonnes pratiques
que faire si le contrôle de l'identité est complexe ?

1. ÉTABLIR UN DIALOGUE DE CONFIANCE

→ Expliquez clairement à l'usager pourquoi la vérification est importante.
→ Adoptez une posture bienveillante et sans jugement pour lever les réticences.

2. RECUEILLIR UNE ATTESTATION SUR L'HONNEUR

→ Proposez à l'usager de rédiger une déclaration attestant de son identité.
→ Aidez-le à compléter ce document si nécessaire.

3. DEMANDER UNE ATTESTATION D'UN TIERS DE CONFIANCE

→ Travailleur social, éducateur, famille ou association peuvent confirmer l'identité de l'usager.
Cette attestation doit être datée, signée et conservée dans le dossier.

4. UTILISER DES DOCUMENTS SECONDAIRES

→ Courriers administratifs récents, carte Vitale, Etc. tout document officiel mentionnant l'identité.
⚠ *Attention à la fiabilité et à la mise à jour de ces documents.*

5. RECOURIR À DES RESSOURCES INSTITUTIONNELLES

En fonction des dispositifs locaux, solliciter l'ARS, la préfecture ou d'autres partenaires pour appuyer la démarche.

Utiliser, si possible, les téléservices sécurisés (ex. INSi) pour croiser les informations.

6. DOCUMENTER LA SITUATION

→ Noter précisément les démarches entreprises et les difficultés rencontrées dans le dossier. Informer le référent identitovigilance pour suivi.

7. ACCOMPAGNER L'USAGER DANS SA RÉGULARISATION

→ Orienter vers les services administratifs compétents (mairie, préfecture).
→ Proposer un soutien dans les démarches de demande ou renouvellement de pièces d'identité.

Points d'attention

- Ne pas exclure un usager faute de justificatif, mais adapter la prise en charge.
- Respecter la confidentialité et le secret professionnel.
- Toujours agir dans le cadre du RGPD et des recommandations CNIL.

Annexe 4.2.4 - Fiche bonnes pratiques comment auto évaluer l'identitovigilance au sein de ma structure ?

→ Sécuriser l'identification des usagers tout au long du parcours coordonné, assurer l'échange fiable d'informations entre les professionnels et éviter les erreurs (doublons, mauvaises orientations, confusion entre usagers).

SYSTÈME DE NOTATION

Chaque axe contient plusieurs critères. Attribution d'une note (Oui = 2 points Partiel = 1 point, Non : pas de point) par critère et en fonction de la somme obtenue, calculez le score global en pourcentage.

AXE	CRITÈRE	EVALUATION	SCORE	COMMENTAIRE - ACTION CORRECTIVES
QUALITÉ DES DONNÉES	Un document fiable d'identité est systématiquement demandé	☐ Oui ☐ Partiel ☐ Non		
	Les identités sont saisies conformément à l'état civil	☐ Oui ☐ Partiel ☐ Non		
OUTIL DE COORDINATION	L'INS est récupérée via INSi quand c'est possible	☐ Oui ☐ Partiel ☐ Non		
	Aucune INS n'est qualifiée sans pièce justificative	☐ Oui ☐ Partiel ☐ Non		
	Les doublons sont recherchés avant toute création de dossier	☐ Oui ☐ Partiel ☐ Non		
	Les échanges de données sont sécurisés	☐ Oui ☐ Partiel ☐ Non		

INFORMATION	L'usager est informé sur l'usage de ses données	☐ Oui ☐ Partiel ☐ Non		
PRATIQUES PROFESSIONNELLES	Les anomalies sont tracées ` et signalées	☐ Oui ☐ Partiel ☐ Non		
	Les professionnels disposent de consignes claires	☐ Oui ☐ Partiel ☐ Non		
GOUVERNANCE	Un référent identitovigilance est nommé	☐ Oui ☐ Non		
	Une procédure est rédigée et diffusée	☐ Oui ☐ Non		
FORMATION ET CULTURE SÉCURITÉ	Une formation à l'identitovigilance est prévue régulièrement	☐ Oui ☐ Non		
SCORE GLOBAL (%)				

INTERPRÉTATION DES RÉSULTATS

SCORE GLOBAL (%)	NIVEAU DE MATURITÉ	SIGNIFICATION	RECOMMANDATION
80 – 100 %	Grandement atteint	Les pratiques sont bien mises en œuvre, maîtrisées et régulièrement actualisées.	Poursuivre les bonnes pratiques
60 – 79 %	Pratiquement atteint	Les actions sont en place mais encore incomplètes ou inégalement appliquées.	Cibler des actions d'amélioration spécifiques
40 – 59 %	Partiellement atteint	Des démarches existent, mais restent peu formalisées ou peu suivies	Mettre en œuvre un plan de renforcement structuré
< 40 %	Non atteint	L'identitovigilance est peu ou pas prise en compte, avec un fort risque d'erreur.	Agir en priorité : mobiliser les équipes, formaliser les procédures de base.

Annexe 4.3 - Fiche de signalement d'anomalie d'identité

1. INFORMATIONS SUR L'USAGER

Nom de naissance : _____

Prénoms : _____

Date de naissance : _____ /_____ /_____

Lieu de naissance : _____

Sexe : ☐ Masculin ☐ Féminin ☐ Autre

2. DESCRIPTION DE L'ANOMALIE CONSTATÉE

☐ Absence de pièce justificative
☐ Incohérence entre documents
☐ Doublon
☐ Données erronées
☐ Impossibilité de qualifier l'INS
☐ Autres (préciser) : _____

3. ACTIONS RÉALISÉES

☐ Vérification des documents d'identité présentés
☐ Recherche de doublons dans le système
☐ Consultation du téléservice INSi
☐ Demande d'informations complémentaires à l'usager
☐ Signalement au référent identitovigilance
☐ Autres (préciser) : _____

4. IMPACT POTENTIEL DE L'ANOMALIE

☐ Risque d'erreur dans la prise en charge
☐ Risque de non-conformité réglementaire
☐ Risque de violation de la confidentialité
☐ Autres (préciser) : _____

5. PERSONNE AYANT DÉTECTÉ L'ANOMALIE

Nom / Prénom : _____
Fonction : _____
Date et heure : ____ / ____ / _____ – ____ : ____

6. SUITE DONNÉE (À REMPLIR PAR LE RÉFÉRENT IDENTITOVIGILANCE)

.....
.....
.....
.....
.....

Signature du professionnel signalant :

Note : Cette fiche doit être conservée conformément à la politique de conservation des données de la structure et traitée dans le respect du RGPD.

Annexe 4.4 - Checklist – Bonnes pratiques en identitovigilance

1. IDENTIFICATION DE L'USAGER

☐ Je demande systématiquement une pièce d'identité officielle (CNI, passeport)
☐ Je vérifie les informations exactes

- ☐ Nom de naissance
- ☐ Tous les prénoms dans l'ordre
- ☐ Date de naissance complète
- ☐ Lieu de naissance
- ☐ Sexe

☐ Je note le nom d'usage uniquement s'il figure sur le document

2. SAISIE DES DONNÉES

☐ Je saisis l'identité sans abréviation, ni inversion
☐ Je respecte l'orthographe et l'ordre des prénoms
☐ Je vérifie l'absence de doublon ou collision avant de créer un nouveau dossier

3. UTILISATION DE L'INS (IDENTITÉ NATIONALE DE SANTÉ)

☐ Je récupère l'INS via le téléservice INSi, si disponible
☐ Je ne modifie jamais manuellement une identité qualifiée
☐ Je signale toute anomalie ou écart entre les données INS et les pièces

4. SÉCURITÉ DES ÉCHANGES

☐ J'utilise uniquement les adresses mails professionnelles pour transmettre des données
☐ Je protège les pièces jointes si besoin (mot de passe, format sécurisé)
☐ Je supprime les mails contenant des données personnelles une fois traités

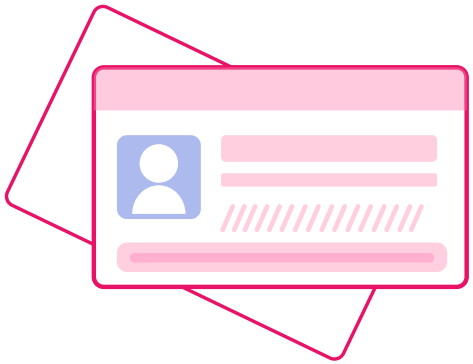
5. INFORMATION ET ACCOMPAGNEMENT

☐ J'explique à l'usager pourquoi l'identification fiable est importante
☐ J'informe sur la confidentialité et la protection des données
☐ Je propose de l'aide pour obtenir un justificatif si besoin

6. EN CAS D'ANOMALIE OU DE DOUTE

☐ Je ne poursuis pas l'enregistrement si l'identité est incertaine
☐ Je contacte le référent identitovigilance
☐ Je documente la situation dans le dossier ou via la fiche de signalement

Annexe 4.5 - fiche d'information usager
Pourquoi vous demande-t-on vos papiers d'identité ?



→ Pour garantir votre sécurité et la qualité de votre accompagnement.

POUR VOUS IDENTIFIER PRÉCISÉMENT

Chaque personne est unique. Vos papiers d'identité (carte d'identité, passeport, Etc.) permettent de confirmer qui vous êtes, afin d'éviter toute confusion avec une autre personne.

POUR PROTÉGER VOS DONNÉES PERSONNELLES

En vérifiant votre identité, nous évitons que vos informations confidentielles ne soient communiquées à quelqu'un d'autre par erreur.

POUR ASSURER LA BONNE COORDINATION DES SOINS ET SERVICES

Une identification fiable permet aux différents professionnels qui vous accompagnent de partager vos informations de manière sécurisée et efficace.

POUR RESPECTER LA LOI

La réglementation vous protège, et nous impose de vérifier votre identité afin d'assurer la qualité et la sécurité des services.

SI VOUS N'AVEZ PAS DE PAPIERS D'IDENTITÉ

N'hésitez pas à nous en parler. Nous sommes là pour vous accompagner et trouver ensemble une solution.

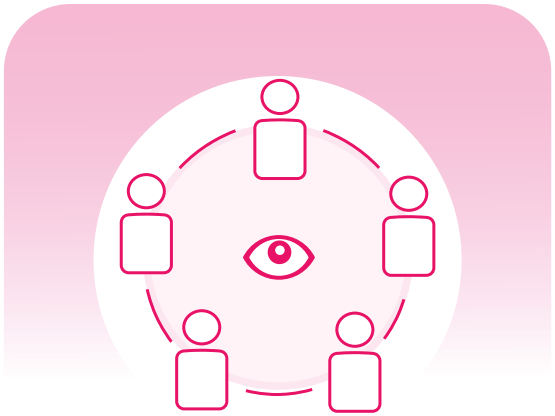
Vos données sont traitées avec confidentialité et respect, conformément à la loi.

CONCLUSION

L'identitovigilance est un levier essentiel pour la sécurité des parcours en santé des usagers.

Elle repose sur :

UNE VIGILANCE COLLECTIVE



UN RESPECT STRICT DES RÈGLES

UNE ORGANISATION ADAPTÉE

Ce guide vous accompagne dans la mise en œuvre concrète de ces bonnes pratiques.

https://www.facs-occitanie.fr/