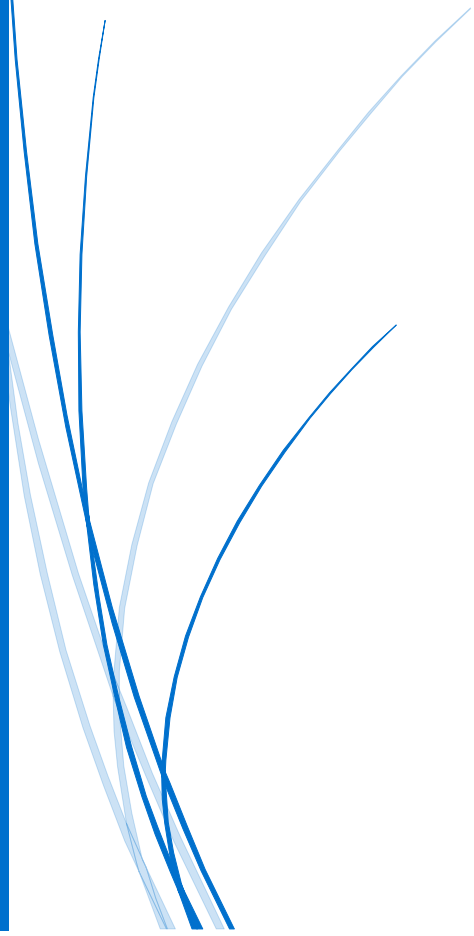
03/01/2025

Charte d'identitovigilance



Référente Identitovigilance : Malvina HARO

V1

Table des matières

CHARTE D'IDENTITOVIGILANCE
ADSCE

1. INTRODUCTION

L'identitovigilance est définie comme l'organisation et les moyens mis en œuvre pour fiabiliser et sécuriser l'identification de l'usager à toutes les étapes de sa prise en charge. Elle concerne :

- l'élaboration de documents de bonnes pratiques relatifs à l'identification de l'usager ;
- la formation et la sensibilisation des acteurs sur l'importance de la bonne identification des usagers à toutes les étapes de leur prise en charge ;
- l'évaluation des risques et l'analyse des événements indésirables liés à des erreurs d'identification
- l'évaluation des pratiques et de la compréhension des enjeux par l'ensemble des acteurs concernés (professionnels, usagers, correspondants externes).

Elle s'applique à toutes les étapes de prise en charge de l'usager en termes :

- d'identification primaire qui vise à attribuer une identité numérique unique à chaque usager dans le système d'information ;
- d'identification secondaire qui permet de garantir que le bon soin ou accompagnement est administré au bon usager.

La charte d'identitovigilance a pour objet de formaliser la politique conduite par **l'ADSCE** pour bien identifier les usagers pris en charge afin de garantir leur sécurité tout au long de leur parcours. Elle définit l'organisation et les moyens mis en œuvre ainsi que les règles à respecter par l'ensemble des professionnels de l'établissement. Elle traite également des droits et devoirs des usagers qui sont également pleinement parties prenantes de leur propre sécurité.

Cette charte est révisée :

- tous les 3 ans ;
- en cas d'évolution réglementaire ;
- en cas d'évolution des outils, des pratiques, du contexte local, des organisations…

2. POLITIQUE D'IDENTITOVIGILANCE

1. Définition et objectifs

La maîtrise de l'identification des usagers est un enjeu majeur pour garantir la qualité et la sécurité de leur prise en charge. L'identitovigilance représente l'ensemble des moyens organisationnels et techniques mis en œuvre pour disposer d'une identification unique, fiable et partagée de l'usager afin d'éviter les risques d'erreurs tout au long de son accompagnement.

Les règles définies par le *Référentiel national d'identitovigilance* (RNIV) s'imposent à l'ensemble des acteurs, qu'ils soient professionnels médicaux, paramédicaux, éducatifs, administratifs, ou usagers.

Leur respect est un prérequis pour la sécurisation de l'échange et du partage d'informations de santé et des accompagnements réalisés au sein de la structure ou en relation avec les correspondants externes, dans le respect de la réglementation en vigueur.

La politique d'identitovigilance est élaborée par une instance de pilotage dédiée qui réunit des représentant de la direction, du système d'information, de la démarche qualité et le référent en identitovigilance de la structure. Elle a fait l'objet d'une concertation avec les représentants des usagers du Conseil de la vie sociale.

2. Engagement de la structure

L'ADSCE accorde une importance particulière à la fiabilisation de l'identification de l'usager qu'il considère comme un acte de soin et d'accompagnement à part entière. Elle s'engage à mettre en place les moyens humains, techniques et organisationnels nécessaires afin de pérenniser les bonnes pratiques dans ce domaine.

La politique d'identitovigilance menée par la structure poursuit les objectifs suivants :
- améliorer la qualité et la sécurité des prises en charges et accompagnements ;
- renforcer la culture de sécurité des professionnels ;
- favoriser le respect des bonnes pratiques d'identification des usagers ;
- déployer l'INS dans tous les usages, en conformité avec les attendus RNIV ;
- réduire le risque d'erreur en termes d'identification de la personne prise en charge et de partage de l'INS ;
- s'assurer qu'une identité numérique, et une seule, correspond à chaque usager pris en charge au sein de la structure afin de garantir que l'ensemble des informations qui le concernent sont accessibles ;
- sécuriser les échanges d'informations personnelles de santé avec les correspondants extérieurs, dans le respect des droits de l'usager et des normes d'interopérabilité…

Cette politique est définie en conformité avec les règles de bonnes pratiques établies par le RNIV (volet 3 spécifique aux structures non hospitalières).

3. Le périmètre d'action de la politique

a. Mode d'accompagnements

La politique d'identification de l'usager s'applique à tous les modes de prise en charge et d'accompagnements présents et proposés par **l'ADSCE** :

- Livraison de repas
- Accompagnement, aide et services aux domiciles
- Soins à domicile

b. Acteurs concernés

L'usager est directement concerné par son identification et doit être, chaque fois que possible, acteur de sa sécurité dans ce domaine.

Les professionnels concernés sont ceux qui prennent en charge directement l'usager et ceux qui interviennent sur tout ou partie des données médico-administratives de l'usager (identification primaire ou secondaire) :

- Salariés administratifs (de chaque antenne) : direction, cadres, cadres de santé, responsables de secteur, assistantes de secteur, agents d'accueil.
- Salariés intervenants : aides à domicile, aides-soignants, infirmiers de suivi.

c. Système d'information

La politique d'identitovigilance concerne l'ensemble des outils gérant des données personnelles relatives aux usagers mises en œuvre au sein de **l'ADSCE,** qu'elles soient ou non alimentées par le référentiel d'identités.

Les applications informatiques partageant des données de santé nominatives sont hébergées en externe auprès d'un fournisseur habilité « hébergement données de santé ».

3. GOUVERNANCE DE L'IDENTITOVIGILANCE

L'ADSCE met en place plusieurs niveaux de gouvernance en cohérence avec les préconisations du RNIV 3 :

- un niveau stratégique appelé **Comité de pilotage de l'identitovigilance (COPIL)** (direction, DPO, référent identitovigilance local)
- un niveau opérationnel, représenté par le référent en identitovigilance et notre correspondant local.

4. Le référent en identitovigilance

Le référent local en identitovigilance est désigné par le directeur de l'établissement. Il est membre de droit du COPIL.

Il est l'animateur principal de la thématique au niveau de l'établissement. À ce titre, il :

- est l'interlocuteur privilégié de la direction de l'établissement, du COPIL et de l'ensemble du personnel pour toutes les problématiques liées à l'identification de l'usager ;
- participe à l'élaboration de la politique d'identification des usagers ;
- assure la veille réglementaire et technique en matière d'identitovigilance, en lien avec les référents régionaux ;
- s'assure de l'adéquation et de la mise en œuvre du plan d'action
- participe au choix des outils et donne un avis d'expert sur leur conformité aux exigences des référentiels (RNIV, guide d'implémentation de l'INS…) et leur adéquation aux besoins de l'établissement, structure ou service en termes d'identification de l'usager ;
- participe à la formalisation et à l'actualisation des documents relatives à l'identification des usagers ;
- participe à la gestion des risques *a priori* et *a posteriori* ;
- participe à la formation et à la sensibilisation du personnel en matière d'identitovigilance ;
- supervise le maintien de la qualité du référentiel d'identités de **l'ADSCE,** en particulier pour la détection et le traitement des anomalies (doublons, collisions, erreurs liées à l'INS) ;
- est responsable de la diffusion et de la gestion des alertes d'identitovigilance internes et externes à la structure ;
- assure le suivi et l'analyse des indicateurs d'identitovigilance définis par le COPIL ;
- assure la communication interne et externe autours de l'identitovigilance ;
- participe à l'animation régionale par le biais de sa participation au comité consultatif régional s'il existe ;
- rend compte à la direction de l'établissement de l'ensemble de ses activités, de toute difficulté rencontrée et des problématiques relatives à l'identitovigilance survenant dans son établissement.

5. Les correspondants en identitovigilance

- **Correspondants en identitovigilance internes**

Le COPIL, peut choisir de désigner des correspondants en identitovigilance pour accompagner le référent dans ses missions et assurer le relais des décisions dans les différents secteurs d'activité. Ils sont également chargés de faire remonter les difficultés rencontrées par les acteurs de terrain.

Ils participent aux actions de formation et de sensibilisation de la structure en matière d'identitovigilance et peuvent être invités aux réunions du COPIL. La liste des correspondants en identitovigilance est communiquée dans chaque service.

Correspondants en identitovigilance externe :

Aurélia BASSET

Cheffe de projets & Référente Régionale en Identitovigilance
GCS e-Santé Bretagne
21 place Duguesclin, 22000 St Brieuc
06 15 93 72 93 | 02 96 33 59 07

aurelia.basset@esante-bretagne.fr - www.esante-bretagne.fr

Les structures partenaires sont invitées à identifier des correspondants en identitovigilance et à transmettre leurs coordonnées au référent en identitovigilance. Ils ont pour objet de faciliter la mise en commun des règles d'identitovigilance mais aussi de participer au signalement et au traitement des erreurs dans le cadre des données de santé échangées. Les coordonnées des correspondants externes sont disponibles

4. DEFINITIONS ET TERMINOLOGIE

L'objet de ce chapitre est de rappeler la signification des termes techniques utilisés dans l'établissement dans le domaine de l'identification de l'usager. Les termes employés en identitovigilance sont définis dans *l'annexe II du volet socle du RNIV 1, Principes d'identification des usagers communs à tous les acteurs de santé*. Il n'en sera précisé que certains dans cette charte qui ont une importance toute particulière en termes de qualité et de sécurité de l'accompagnement.

1. Identification

Identifier une personne consiste à disposer des informations nécessaires et suffisantes pour ne pas confondre cette personne avec une autre. Cela consiste à recueillir les informations (traits) représentant une personne physique pour l'identifier de façon unique. Ces traits d'identification sont utilisés comme critères pour rechercher l'usager dans le système d'information. Ils concourent à la sécurité de sa prise en charge et de l'accompagnement.

2. Identité et identifiant numériques

Identité numérique : représentation de l'identité d'une personne physique dans un système d'information. L'identité numérique est composée d'un ou plusieurs identifiant(s) numérique(s) et de traits d'identification.

Identifiant numérique : séquence de caractères qu'un ou plusieurs domaines d'identification utilisent pour représenter une personne et lui associer des informations dans le cadre de sa prise en charge.

Identité nationale de santé (INS) : ensemble de traits constituant l'identité sanitaire officielle d'un usager de la santé, tels qu'ils sont enregistrés dans des bases nationales. L'identité nationale de santé est composée de 5 traits stricts de références (nom de naissance, prénom(s), sexe, date de naissance, code du lieu de naissance (commune ou pays pour un usager nés à l'étranger), d'un matricule INS qui a pour valeur le NIR (numéro d'identification au répertoire des personnes physiques) ou le NIA (numéro d'identification d'attente) de l'individu.

3. Domaine d'identification et de rapprochement

Le domaine d'identification (DI) est le périmètre au sein duquel chaque usager est représenté par un seul IPP. Chaque DI identifie l'usager de façon propre avec un identifiant numérique interne.

Le rapprochement est l'opération qui consiste à créer un couple d'identités issues de deux DI distincts et correspondant à une même personne physique. Les deux domaines d'identification sont alors dits « domaines rapprochés ».

4. Traits d'identification

Les traits d'identification sont les informations définies dans un système d'information comme constituants de l'identité numérique d'un usager.

On distingue :

- les traits stricts : ce sont les informations de référence qui caractérisent l'identité officielle de l'usager ; elles permettent de référencer les données de santé partagées et de fiabiliser les rapprochements d'identités numériques entre structures. Les traits stricts sont stables dans le temps pour la très grande majorité des usagers.
- les traits complémentaires : ce sont des données qui apportent d'autres informations utiles à la prise en charge de l'usager mais qui sont plus variables dans le temps.

5. Statuts des identités

Les statuts de l'identité sont utilisés pour attribuer un niveau de confiance à l'identité numérique. On distingue 4 statuts :

- Identité provisoire : statut de plus bas niveau de confiance d'une identité, il correspond à une identité créée localement sans contrôle de cohérence avec un dispositif d'identification de haut niveau de confiance. Il s'agit du statut attribué par défaut à toute identité nouvellement créée localement.
- Identité validée : ce statut correspond à une identité créée localement dont la cohérence a été contrôlée à l'aide d'un dispositif d'identification de haut niveau de confiance. L'attribution du statut identité validée est une action manuelle et volontaire du professionnel.
- Identité récupérée : Ce statut caractérise une identité créée ou modifiée par appel au téléservice INSi et récupération de l'INS, les traits de l'identités sont ceux de l'INS. Toutefois le contrôle de cohérence de ces traits avec ceux présents sur un dispositif d'identification de haut niveau de confiance n'a pas été réalisé.
- Identité qualifiée : statut de plus haut niveau de confiance, d'une identité et seul statut permettant l'utilisation du matricule INS (et de l'OID) pour référencer, échanger et partager des données de santé, il correspond à une identité créée ou modifiée par appel au téléservice INSi et récupération de l'INS et dont la cohérence a été contrôlée à l'aide d'un dispositif d'identification de haut niveau de confiance.

6. Doublons, fusions et collisions

Le doublon d'identités numériques correspond à l'identification d'une même personne sous au moins deux identifiants numériques différents dans un même domaine d'identification (DI). Les informations d'un même usager sont donc réparties dans plusieurs dossiers différents qui ne communiquent pas entre eux. L'équipe soignant ne dispose donc pas de l'ensemble des informations qui peuvent être nécessaires à la prise en charge.

Lors du dépistage d'un doublon, celui-ci est tout d'abord qualifié de doublon potentiel. L'étude des deux dossiers permet de qualifier ce couple de doublon avéré s'il s'agit réellement d'un doublon ou d'homonymes dans le cas contraire.

La fusion correspond au traitement des doublons avérés ; elle consiste à regrouper toutes les informations d'un même individu sous un identifiant numérique unique. l'IPP conservé est alors appelé IPP maitre et l'IPP fusionné, l'IPP esclave ou fantôme selon les systèmes d'informations.

La collision correspond à la présence, sous un même identifiant numérique, d'informations issues de 2 usagers différents. On distingue la collision primaire qui peut résulter d'une erreur de choix de dossier usager lors d'une venue, être la conséquence de l'utilisation frauduleuse d'une identité par un autre individu ou être la conséquence d'une fusion réalisée avec des critères insuffisants. Ces situations de non-qualité sont particulièrement difficiles à corriger.

5. LA GESTION DE L'IDENTITE

1. Le domaine d'identification = ARCAD

L'ADSCE dispose d'une interface unique d'identité pour toutes les applications participant au processus de soins et d'accompagnement. L'ensemble des applications est alimenté en identité par les logiciels spécifiques (ERP). La cartographie applicative des droits d'accès aux logiciels et des différents dossiers sont présents sur le serveur.

2. Les identifiants utilisés dans l'établissement

Les identifiants numériques utilisés dans l'établissement sont :

- L'identifiant N°client ; Numéro de matricule INS.
- Numéro de session Arche MC2

3. Les lieux de création de l'identité

Les lieux de création d'identité ainsi que les fonctions des personnels dans l'établissements sont décrits dans le tableau suivant.

lieux	Quand	Fonction des personnels
Au domicile du bénéficiaire ou dans le service sur chaque antenne.	A toutes nouvelles demandes (prospects et usagers) ou modification particulière	Accueil Responsables de secteur Cadres IDE

4. Les traits d'identification

L'ADSCE respecte les exigences du RNIV en matière de traits d'identification. Les traits d'identification utilisés sont les suivants :

a. Traits stricts

- Nom de naissance ;
- Premier prénom d'état civil ;
- Liste des prénoms de naissance figurant sur un titre officiel d'identité ;
- Date de naissance ;
- Sexe ;
- Lieu de naissance, sous forme de code INSEE de la commune (pour les usagers nés en France) ou du pays (pour les autres) ;
- Matricule INS (toujours associé à son OID1).

b. Traits complémentaires

La saisie des traits complémentaires identifiés par une * est rendue obligatoire par le RNIV.

- Nom utilisé* (saisie obligatoire si différent du nom de naissance) ;
- Prénom utilisé* (saisie obligatoire si différent du premier prénom de naissance) ;
- Commune de naissance ;
- Adresse de résidence de l'usager ;
- Numéros de téléphone (portable et fixe) ;
- Adresse(s) courriel de contact ;
- Nom des personnes en relation (parents, enfant, conjoint, personne de confiance, personne à prévenir…) ;
- Nom et coordonnées de la personne de confiance ;
- Nom et coordonnées du médecin traitant ;
- Autres professionnels de santé impliqués dans la prise en charge ;
- Profession ;
- Type de document d'identité présenté (attention, il ne faut pas saisir le numéro de la pièce)
- …etc.

c. Politique de la structure concernant la saisie des noms et prénoms utilisés

L'ADSCE a fait le choix de :

Recopier à l'identique les éléments d'identité présents sur la pièce d'identité présentée par l'usager.

- saisir un nom utilisé s'il est mentionné sur la pièce d'identité, y compris si l'usager ne le souhaite pas. L'usager sera alors informé qu'il lui appartient de faire modifier sa pièce d'identité ;
- saisir un prénom utilisé uniquement si celui-ci est explicitement mentionné sur la pièce d'identité :
    - ce prénom fait partie des prénoms de naissance (article 57 du code civil, tout prénom de naissance peut être utilisé comme prénom usuel),

Si coordonnées communiquées par Tiers par téléphone ou en présentiel => pas de traits stricts complets => saisie des données minimales obtenues par la personne qui accueille qui seront complétées lors de l'évaluation soit par le coordinateur ou un autre professionnel sur la base des données saisies à l'écrit.

Traits stricts demandé lors de la création de l'identité à l'oral.

Contrôle des traits avec la pièce d'identité si enregistrement en présentiel

- le champ « nom utilisé » n'est renseigné que si l'usager utilise un nom différent de son nom de naissance ;
- le champ « prénom utilisé » n'est renseigné que si l'usager utilise un prénom différent de son premier prénom de naissance.

5. Recherche, création, qualification d'une identité

a. Accueil de l'usager

Tout professionnel de l'accueil demande à l'usager de décliner son identité par question ouverte y compris si l'usager présente une pièce d'identité.

Cette pratique permet d'améliorer le dépistage des erreurs (erreur de sélection d'une pièce d'identité par l'usager s'ils en possèdent plusieurs – celles des enfants mineurs par exemple – et des utilisations frauduleuses d'identité).

b. Recherche d'une identité

Conformément au RNIV, la recherche d'une identité est réalisée par la saisie du Nom de naissance ou d'usage (indiqué par l'usager).

Le système d'information permet la recherche d'une chaine de caractères à la fois dans les champs nom de naissance et le nom utilisé pour le nom et dans les champs prénoms de naissance et prénom utilisé pour le prénom, et est insensible à la présence de tiret ou d'apostrophe.

c. Création d'une identité

Conformément au RNIV, les traits obligatoires pour créer une identité sont :

- le nom de naissance ;
- le nom utilisé (à ne conserver que si la structure pratique du double nommage sur le champ nom utilisé)
- le premier prénom de naissance ;
- le prénom utilisé (à ne conserver que si la structure pratique le double nommage sur le champ prénom utilisé)
- le sexe ;
- la date de naissance ;
- le code INSEE du lieu de naissance : le système d'information de la structure propose automatiquement un code de lieu de naissance si la ville et/ou le code postal du lieu de naissance sont saisis.

Ces traits stricts sont complétés par :

- la liste des prénoms de naissance ;
- le matricule INS

dès que l'appel au téléservice a pu être réalisé pour les usagers éligibles.

Et par les traits complémentaires suivants :

- adresse postale
- adresse courriel

- numéro de téléphone ;
- médecin traitant
- personne à prévenir
- personne de confiance…

Le processus détaillé de création d'une identité est décrit dans une procédure. Seuls les éléments structurants sont repris ici.

Les règles de saisie des identités

Les champs nom de naissance, nom utilisé, premier prénom, liste des prénoms, prénom utilisé sont saisis **en majuscule sans caractères accentués ou diacritiques**. **Tirets et apostrophes sont conservés.**

L'utilisation de l'opération de récupération du téléservice INSi

L'établissement a fait le choix de n'appeler le téléservice que si l'identité de l'usager est au statut identité validée.

Création des identités sur temps de travail par les professionnels administratif et/ou professionnels de santé

- Les professionnels présents créent une identité locale. La récupération de l'INS est réalisée par le responsable de secteur après réalisation d'un contrôle de cohérence entre l'identité numérique locale et les traits présents sur une pièce d'identité de haut niveau de confiance.

d. Les attributs d'identité

L'établissement utilise les attributs :

- identité douteuse : cet attribut est utilisé lors d'une suspicion d'utilisation frauduleuse d'identité par un usager (usurpation d'identité) ;
- identité fictive : cet attribut permet de caractériser une identité numérique ne reposant pas sur les traits réels de l'usager pris en charge (usagers incapables de décliner leur identité, anonymat par exemple) ;
- identité homonyme : pour attirer l'attention des professionnels sur la présence d'identités approchantes dans le référentiel identité.

e. Le processus de validation des identités et de qualification de l'INS

Pour les bénéficiaires déjà accompagnés : La validation des identités est réalisée en back office par le responsable de secteur après réalisation d'un contrôle de cohérence entre l'identité numérique et l'identité présente sur la pièce d'identité.

Pour les nouvelles entrées : La validation est réalisée au vu d'une pièce d'identité de haut niveau de confiance par le personnel qui crée ou modifie l'identité. L'usager doit avoir présenté un dispositif d'identification à haut niveau de confiance.

Avant cette opération de validation, il est demandé à l'usager ou à son accompagnant de contrôler l'exactitude des informations saisies.

Les dispositifs d'identification à haut niveau de confiance conformément au RNIV sont les suivants :

- carte nationale d'identité pour les usagers français et les ressortissants de l'Union Européenne
- passeport ;
- titre de séjour ;

pour les mineurs ou personnes de plus de 60 ans , livret de famille ou extrait d'acte de naissance accompagné de la pièce d'identité du responsable légal

- dispositif d'identification électronique de niveau substantiel.

f. Les identités particulières

Sans objet

g. Identification primaire sans présence physique de l'usager

Sans objet

6. Le maintien de la qualité du référentiel identité

Le maintien de la qualité du référentiel identité est sous la responsabilité du COPIL.

Tous les professionnels sont formés et incités à la déclaration des anomalies :

- erreur d'identité ;
- doublon potentiel ;
- collision potentielle ;
- erreur d'attribution d'une INS.

Le signalement et le traitement des anomalies sont formalisés dans une procédure à disposition des personnels.

- les anomalies qui doivent être signalées ;
- le moyen de signalement (mail, outil dédié type logiciel d'identitovigilance, portail intranet de l'établissement, fax…) ;
- les éléments indispensables au signalement (qui peuvent être présents dans un formulaire à remplir) ;
- les suites données au signalement ;
- l'information rétroactive des personnels.

La procédure de traitement des anomalies doit comporter :

- le type d'anomalies traitées (collision, doublon, erreur sur une identité, erreur sur une INS…) ;
- les acteurs en charge du traitement ;
- les vérifications réalisées au cours du traitement ;
- la politique de fusion en termes d'identité numérique à conserver (IPP le plus ancien, dossier le plus riche, identité de plus haut niveau de confiance…)
- la traçabilité des actions le temps du traitement (la fusion est-elle réalisée au cours de l'hospitalisation ou après la sortie ?)
- l'information des personnels et services de l'établissement ;
- l'information des partenaires hors du domaine d'identification (sous-traitants par exemple), en particulier si les modifications ne peuvent être propagées par des flux d'interopérabilité ;
- la répercussion des fusions et/ou des modifications d'identités dans les outils incomplètement ou non interfacés ;
- la prise en compte du traitement des collisions dans les outils métiers (PACS, DPI…) en précisant en particulier l'identification de l'acteur en charge (correspondant d'identitovigilance du service par exemple) ;
- la réimpression éventuellement nécessaire de documents (bracelet, étiquettes…)

7. Droits d'identification

Coordination et d'orientation	Administratif ou appui à l'organisation de l'accompagnement SMS	Accompagnement SMS à la vie sociale, professionnelle et éducative	Accompagnement SMS au soin	Encadrement et organisation de l'accompagnement SMS
Coordination dans les DAC, dans les ESMS (CLIC de niveau 3, Communautés 360, APV, SAMSAH, ...), dans les MDPH, ...	Accueil, information, secrétariat, appui aux démarches administratives, accès aux droits	Auxiliaire de vie sociale, Accompagnant éducatif et social (AES), Assistant de vie dépendance et handicap (AVDH), Aide à domicile, Technicien de l'intervention sociale et familiale, Conseiller en économie sociale et familiale (CESF), Conseiller en insertion professionnelle (CIP), Moniteur éducateur, éducateur de jeunes enfants, éducateur spécialisé, éducateur technique spécialisé, moniteur d'atelier (ESAT et EA), responsable de production (ESAT et EA), Animateur	Paramédicaux, AMP, aide soignant, auxiliaire de puériculture, psychothérapeute, assistant de soin en gérontologie, neuropsychologue	Responsable de secteur, gestionnaire de secteur, chef de service, directeur/trice d'ESMS, directeur/trice adjoint

6. FIABILISATION DE L'IDENTIFICATION SECONDAIRE

8. Identification de l'usager lors des prestations d'accompagnement et de soins

Chaque professionnel habilité, avant la réalisation d'un accompagnement ou d'un soin, vérifie l'identité de l'usager s'il est communicant, en lui posant des questions ouvertes sur a minima :

- son nom de naissance ;
- son premier prénom de naissance ;
- sa date de naissance.

Si l'usager est non communicant, l'identité est vérifiée sur le dispositif d'identification ou communiqué par un tiers.

La cohérence de l'identité est vérifiée avec les supports disponibles (écrits professionnels, étiquettes…)

La vérification de l'identité de l'usager par le professionnel est tracée dans le dossier. L'établissement peut décrire ici les modalités de traçabilité ou renvoyer à la procédure de qualification de l'INS (cf logigramme).

Une procédure est disponible dans la gestion documentaire.

9. Identification des documents du dossier de l'usager

L'ADSCE dispose d'une organisation et de moyens lui permettant de garantir que tous les éléments du dossier de l'usager sont identifiés et de limiter les erreurs lors de la numérisation de documents dans le dossier patient informatisé.

- Le dépôt de documents dans le SI métier est assuré par chaque professionnel qui s'assure que l'identité de l'usager corresponde

7. LA GESTION ELECTRONIQUE DOCUMENTAIRE (GED)

L'ensemble de la documentation, procédures, modes opératoires, enregistrements, relative à l'identitovigilance sont disponibles dans l'outil de gestion documentaire de l'armoire qualité de l'outil.

L'alimentation de la GED est sous la responsabilité du service qualité et DPO.

1. Procédures

Les procédures en vigueur dans l'établissement sont les suivantes :

- Identification primaire lors de l'accueil de l'usager (recherche d'une identité, création d'une identité, attribution d'un niveau de confiance). Cette procédure peut être déclinée éventuellement selon les modalités de réception (Téléphonique, présentiel, mail, les points d'accueil ; courrier …)
- Identification secondaire d'un usager avant tout accompagnement ou soin ;
- Signalement des anomalies liées à l'identité (erreurs d'identité, détection de doublons, collisions, usurpation d'identité, erreur de récupération d'un INS, erreur de vérification d'un INS…) ;
- Prise en charge des anomalies liées à l'identité (correction d'une identité numérique, traitement des doublons, traitement des collisions) ;
- Signaler une suspicion de substitution frauduleuse d'identité ;
- Information des partenaires après détection d'une erreur d'identification d'un usager ;
- Mode de fonctionnement dégradé en cas de panne informatique, notamment en termes de gestion de l'identification primaire et secondaire et de reprise d'activité ;
- Procédure de gestion et de contrôle des bases d'identités des professionnels au sein du SI et la définition des droits d'accès (cette procédure intégrera la gestion des clôtures de compte).

2. Modes opératoires

Sans objet

3. Enregistrements

Les enregistrements suivants sont disponibles dans la gestion documentaire de l'établissement :

- documents réglementaires et techniques (fiches du réseau 3RIV, …) ;
- charte SI ;
- cartographie applicative et schéma des flux ;
- supports de formations ;
- Support de communication et de sensibilisation (affiches, flyers…) ;
- plan d'action ;
- bilan d'activité ;
- cartographie des risques a priori (cotés et hiérarchisés) ;
- tableau de bord des indicateurs ;
- grilles et guides d'évaluations ;
- résultats et analyses d'évaluations ;
- comptes rendus des analyses réalisées suites à la survenue d'évènements indésirables (Retours, d'expérience, …).

8. PILOTAGE

L'ADSCE suit des indicateurs relatifs à l'identification primaire et à l'identification secondaire.

Chaque indicateur dispose d'une carte d'identité disponible dans les solutions métiers, GED ou tout autre support.

Les indicateurs sont rassemblés dans un tableau de bord et sont suivis annuellement. Le tableau de bord des indicateurs tenu à jour par le Référent Identitovigilance

1. Indicateurs d'identification primaire

Les indicateurs listés dans ce chapitre sont les indicateurs proposés.

Les indicateurs suivis dans la structure sont les suivants

- taux d'identités nationales de santé ou INS ;
- taux d'identités au statut identité qualifiée ;
- taux d'identités au statut identité récupérée ;
- taux d'identités au statut identité validée ;
- taux d'identités au statut identité provisoire ;
- taux d'évènements porteurs de risques ayant pour origine une erreur d'identification primaire des usagers.

2. Indicateurs d'identification secondaire

Les indicateurs suivis dans la structure sont les suivants

- taux d'évènements porteurs de risques ayant pour origine une erreur d'identification secondaire des usagers ;
- taux d'évènements indésirables ayant pour origine une erreur d'identification secondaire des usagers ;

3. Formation du personnel

Les indicateurs suivis dans la structure sont les suivants :

- taux de formation du personnel par catégories professionnelles habilités à qualifier les INS ;
- taux de formation du personnel par catégorie spécifique de personnels.

4. Évaluation et amélioration des pratiques professionnelles

L'établissement prévoit dans son plan d'action annuel les évaluations à mettre en œuvre, a minima une évaluation relative à l'identification primaire et deux évaluations relatives à l'identification secondaire.

Intitulé de l'audit	Complet	Flash
IDENTIFICATION PRIMAIRE		
Vérification de l'identité de l'usager (secrétariats sans création d'identité)	✔	✔
Recueil de l'identité lors de l'accueil de l'usager (points de création d'identité)	✔	✔
IDENTIFICATION SECONDAIRE		
Evaluation des règles d'identification lors d'un prélèvement biologique	✔	✔
Exhaustivité du port du bracelet d'identification chez le patient hospitalisé ou en ambulatoire	✔	
Evaluation des règles d'identification de l'usager lors d'un transport interne	✔	✔
Evaluation des règles d'identification de l'usager en imagerie médicale	✔	
Evaluation de l'identification des préparations injectables		✔
Identification de l'usager au moment de l'administration médicamenteuse		✔
Identification de l'usager lors du soin repas		✔

Source :https://grives.sante-paca.fr/

L'analyse est présentée au COPIL, les actions d'amélioration sont validées mises en œuvre par le référent en identitovigilance, le COPIL, le service qualité gestion des risques. Les résultats sont restitués au personnel et disponibles dans la GED.

9. LA GESTION DES RISQUES

1. La gestion des risques a priori

a. La veille réglementaire et technique

Le référent en identitovigilance réalise une veille réglementaire et technique en utilisant les ressources disponibles (liste non exhaustive) :

- utilisation des espaces collaboratifs régionaux en identitovigilance (GCS eSanté Bretagne, UNA Bretagne, Pole excellance Cyber PEC)
- consultation du site de l'Agence du Numérique en Santé ;
- communication des éditeurs ; (Arche MC 2)
- participation des sessions de formations et d'information ; (ACCENS, UNA)

b. Modalités d'attribution et de gestion des droits d'accès informatiques

L'établissement a défini des profils d'accès au système d'informations dépendant de la fonction des personnels. La liste de ces profils est consultable dans la GED.

Les profils d'accès sont mis à jour ou supprimés en fonction des entrées et sorties du personnel.

L'attribution de droits d'accès au système d'information, la gestion des accès et les modalités de contrôles mises en œuvre sont décrites dans la charte informatique.

L'obtention de droit d'accès au système d'information est conditionnée par la signature de la charte d'utilisation des moyens informatiques. Cette charte précise les droits et devoirs de l'utilisateur, répertorie l'ensemble des moyens informatiques et outils numériques mis à disposition des utilisateurs, définit les pratiques autorisées, les mesures de contrôle pouvant être mises en œuvre, les sanctions encourues en cas de non-respect des obligations de la charte.

Tout départ de personnel est signalé auprès de la Direction, le compte est alors immédiatement inactivé.

Conformément à la politique générale de sécurité des systèmes d'information en santé, une revue des droits d'accès est réalisée semestriellement.

La liste des droits d'accès, la matrice des droits sont tenues à jour par le responsable des systèmes d'information.

Les personnels habilités à créer des identités sont formés et évalués avant l'attribution des droits.

c. Traçabilité des actions

L'ensemble des applications informatiques participant à la prise en charge de l'usager disposent de fonctionnalités d'enregistrement horodaté des accès précisant le nom (login), le type d'accès (lecture ou écriture), les documents consultés.

L'ensemble des actions réalisées sur les identités sont tracées, historisées et conservées pendant la durée de vie du dossier.

La structure définit les personnels ayant besoin d'accéder à l'historisation des informations. L'octroi de ces droits d'accès doit être justifié par la finalité

- membre du COPIL
- référent en identitovigilance
- personnels du service informatique…

Des contrôles d'accès aux dossiers sont réalisés :

- ponctuellement sur les dossiers sensibles (dossier de personnels de l'établissement, …) ou en cas de plainte ou de réclamation ou lorsqu'il existe un doute sur le comportement d'un professionnel ou à titre systématique, par exemple pour vérifier l'absence d'intrusion externe dans le système d'information.

d. Fiabilisation des interfaces d'identités

Sans objet

e. Sécurisation de l'identité dans les logiciels non ou incomplètement interfacés

Sans objet

f. Détection des utilisations frauduleuses d'identités

L'établissement porte une attention particulière au risque d'utilisation frauduleuse d'une identité. Les personnels sont formés et mettent en œuvre des contrôles permettant de suspecter une usurpation d'identité. Les usagers sont sensibilisés aux risques encourus lors de l'utilisation frauduleuse d'une identité (affiches présentes aux points d'accueil).

La conduite à tenir devant une suspicion est formalisée et connue des personnels.

- la création d'un dossier provisoire pour ne pas risquer de collision avec un dossier précédent ;
- le signalement interne de l'événement indésirable (cf. Error! Reference source not found.) ;
- l'identification des documents transmis qui n'appartiennent pas à l'usager ;
- l'information des structures et professionnels avec lesquels les données ont été partagées ;
- la suppression de ces documents dans l'outil de partage virtuel utilisé par la structure (si applicable) ;
- la recherche de compléments d'informations ;
- le signalement externe aux parties prenantes (exemples : main courante, dépôt de plainte, alerte adressée à l'Assurance maladie, au médecin traitant, aux sous-traitants, information de l'usager dont l'identité a été empruntée…).

5. La gestion des risques *a posteriori*

L'établissement met en œuvre un système de signalement des événements indésirables, piloté par le responsable et référent en identitovigilance. Il promeut son emploi par l'ensemble des professionnels de l'établissement en priorisant les événements indésirables ayant un impact potentiel sur la sécurité des prestations d'accompagnement et de soins et notamment le signalement des erreurs en lien avec l'identification des usagers. L'établissement communique également auprès de ses partenaires (établissements partenaires, médecins traitants, autres professionnels de santé) pour qu'ils lui signalent les anomalies constatées sur l'identification des usagers.

Les évènements indésirables graves font systématiquement l'objet d'une analyse utilisant une méthodologie adaptée. Les évènements porteurs de risques récurrents sont également analysés en comité de retour d'expérience.

Le référent en identitovigilance et le COPIL sont informés de la survenue d'évènements indésirables, et destinataires des fiches de signalement. Ils participent à leur cotation, leur analyse, à la définition du plan d'action mis en place et à la mise en œuvre des actions.

Les évènements indésirables graves sont signalés sur le portail national de signalement des événements sanitaires indésirables.

Les évènements indésirables signalés, leur analyse permettent de réactualiser périodiquement (tous les ans) la politique d'identitovigilance de l'établissement.

10. LA FORMATION ET LA SENSIBILISATION DES ACTEURS

Tous les personnels de la structure sont formés à l'identitovigilance. La formation est obligatoire pour tous les nouveaux arrivants.

Le référent en identitovigilance organisera des formations à l'identitovigilance pour les nouveaux arrivants dans les six mois suivant l'arrivée

Sensibilisation à l'identitovigilance pour tous les professionnels de la structure une fois par an minimum. Des outils de sensibilisation seront mis à disposition et communiqué à l'ensemble des professionnels (webinaire,newsletters).

La formation dispensée comprend les éléments suivants :

- présentation de la gestion documentaires (principales procédures et organisation de la gestion documentaire) ;
- formation aux bonnes pratiques d'identitovigilance
    - Identitovigilance secondaire avec base d'identitovigilance primaire pour le personnel soignant ;
    - identitovigilance primaire renforcée avec bases d'identitovigilance secondaire pour les professionnels de l'accueil ;
- gestion des risques a priori avec en particulier une présentation des principaux risques identifiés dans l'établissement ;
- gestion des risques *a posteriori* avec en particulier la déclaration des évènements indésirables (quels évènements déclarer, comment déclarer un évènement indésirable, intérêt de déclarer et d'analyser les évènements indésirables).

La formation est tracée dans un listing des personnels formés et traçabilité dans le dossier de formation de chaque personnel). Pour mémoire le taux de personnel formé fait partie des indicateurs d'identitovigilance.

Le plan de formation continue de l'établissement intègre les formations en lien avec l'identitovigilance.

Les personnels suivent une formation de remise à niveau tous les trois ans.

3 sessions de formation à l'identification secondaire et 2 sessions de formation à l'identification primaire sont organisées annuellement. La formation est dispensée par un personnel du COPIL. Les dates sont communiquées aux cadres des services, qui alimentent un fichier d'inscription. Il est obligatoire d'assister à au moins une session tous les trois ans.

Si de mauvaises pratiques du fait d'un professionnel sont identifiées, un point personnalisé est réalisé par le COPIL en présence du responsable hiérarchique si cela est nécessaire.

6. Action de sensibilisation et de communication auprès des professionnels

- affichage dans les services de posters ;
- distribution de flyers de sensibilisation, newsletters
- communication autours des erreurs, des presque accidents ou évènements porteurs de risques, analyse des évènements indésirables…

11. RESPECT DES DROITS DE L'USAGER, INFORMATION SENSIBILISATION

1. Respect du RGPD

L'ADSCE a formalisé, sous l'autorité de son délégué à la protection des données (DPD), la documentation prévue par le Règlement général de protection des données (RGPD

Un document d'information sur l'utilisation de ces services est affiché dans les lieux d'accueil administratif et dans le livret d'accueil de l'établissement. Il précise les principes de partage des données d'identification personnelles dans le cadre régional et les modalités mises en œuvre pour respecter les droits de l'usager. Ce document rappelle en particulier les droits de l'usager :

- d'être informé en cas de traitement automatisé des informations le concernant en particulier de l'utilisation de l'INS par les professionnels de santé pour échanger et partager des données et de l'impossibilité de s'opposer à l'utilisation de l'INS (obligation légale) ;
- d'avoir accès aux informations médicales le concernant ;
- de demander la rectification des données erronées ou périmées ;
- d'avoir la garantie de la confidentialité des informations le concernant…

7. Information et sensibilisation des usagers

L'établissement accorde une attention particulière à l'information des usagers qui doivent être acteurs de leur parcours de soins et d'accompagnement.

L'information est réalisée par le biais d'affiches traitant d'identification primaire disposées dans les points d'accueil et d'affiche traitant d'identification secondaire disposées dans les services de soins et au niveau des lieux de vie collectifs. Le livret d'accueil de la personne accompagnée intègre un chapitre concernant la gestion de l'identité et ses droits d'accès et de modification de ses données.

L'usager est informé au plus tôt des documents qu'il devra présenter lors de sa venue en particulier un dispositif d'identification à haut niveau de confiance :

- les éléments d'information sont présents sur les affiches, dans le livret d'accueil ;

12. ACTUALISATION DE LA CHARTE ET DE LA DEMARCHE D'IDENTITOVIGILANCE

La politique et la charte sont actualisées périodiquement pour prendre en compte :

- les évolutions réglementaires ;
- les résultats des évaluations menées dans l'établissement et les résultats des indicateurs ;
- les évènements indésirables, leur analyse, les plans d'actions mis en place.

13. REFERENCES BIBLIOGRAPHIQUES

Charte d'identitovigilance du GRIVES PACA Accueil - GRIVES (sante-paca.fr)

Charte d'identitovigilance du Comité technique régional d'identitovigilance de Nouvelle-Aquitaine Charte d'identitovigilance | identitovigilance (identito-na.fr)

Arrêté du 27 mai 2021 (Journal officiel du 8 juin 2021) portant approbation des modifications apportées au référentiel « identifiant national de santé» Référentiel national d'identitovigilance

Guide d'implémentation de l'INS à l'usage des éditeurs

Arrêté du 24 décembre 2019 portant approbation du référentiel « Identifiant national de santé »

Décret 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) comme identifiant national de santé

Décret N° 2019-1036 du 8 octobre 2019 modifiant le décret N° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques

comme identifiant national de santé et les articles R. 1111-8-1 à R. 1111-8-7 du code de la santé publique

Décret N° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire

HAS. Manuel certification des établissements de santé pour la qualité des soins. Octobre 2020 Critère 2.3-01 Les équipes respectent les bonnes pratiques d'identification du patient à toutes les étapes de sa prise en charge.

HAS. Amélioration des pratiques et sécurité des soins, la sécurité des usagers. Mettre en œuvre la gestion des risques associés aux soins en ES. Des concepts à la pratique Guide de gestion des risques. Mars 2012.