**KIT DE DEPLOIEMENT DE L’IDENTITOVIGILANCE EN MEDICOSOCIAL**

**FICHES PRATIQUES DE MISE EN ŒUVRE**

Ce document permet de retrouver l’ensemble des fiches pratiques, au nombre de cinq, permettant de mettre en œuvre l’identitovigilance au sein de l’établissement et service médico-social.

[1 Fiche pratique - Gouvernance 2](#_Toc89779396)

[1.1 L’instance de gouvernance 2](#_Toc89779397)

[1.2 Le référent en identitovigilance 3](#_Toc89779398)

[2 Fiche pratique - Identification primaire 5](#_Toc89779399)

[2.1 Notions clés 5](#_Toc89779400)

[2.2 Bonnes pratiques organisationnelles 7](#_Toc89779401)

[2.3 Bonnes pratiques de la création d’une identité numérique 7](#_Toc89779402)

[3 Fiche pratique - Identification secondaire 9](#_Toc89779403)

[3.1 Pourquoi est-ce nécessaire ? 9](#_Toc89779404)

[3.2 Les bonnes pratiques à mettre en œuvre 9](#_Toc89779405)

[4 Fiche pratique – Pilotage du déploiement de l’identitovigilance et de la démarche d’amélioration 11](#_Toc89779406)

[4.1 Sur quelles données s’appuyer ? 11](#_Toc89779407)

[4.2 Quels indicateurs doit-on suivre ? 11](#_Toc89779408)

[4.3 Recueillir et analyser les indicateurs 12](#_Toc89779409)

[5 Fiche pratique - Gestion des risques 13](#_Toc89779410)

[5.1 Notion de gestion des risques 13](#_Toc89779411)

[5.2 Identification des événements indésirables en identitovigilance 13](#_Toc89779412)

[5.3 Typologie des EI relatifs à l'identitovigilance 14](#_Toc89779413)

[5.4 GDR au niveau régional 14](#_Toc89779414)

[5.5 Références utiles 15](#_Toc89779415)

[6 Fiche pratique – Matrice RACI mise en œuvre de l’Identitovigilance dans le secteur médico-social 16](#_Toc89779416)

[7 Glossaire et définitions 18](#_Toc89779417)

# Fiche pratique - Gouvernance

Définir la gouvernance de l’identitovigilance est la première étape de la mise en œuvre de l’identitovigilance. Les grands principes de la gouvernance sont édictés dans le Référentiel national d’identitovigilance (RNIV) mais ils doivent être adaptés à la structure, son activité, sa taille, les caractéristiques de ses usagers et son organisation. Il ne s’agit pas uniquement de mettre en place la gouvernance pour répondre à une exigence réglementaire : la démarche doit être efficiente pour piloter la thématique, mettre en place l’identitovigilance dans la structure et sécuriser les accompagnements.

## L’instance de gouvernance

L’implication de la direction de la structure est impérative. Elle se concrétise par la formalisation de la politique conduite dans ce domaine. La direction détermine les moyens institutionnels, organisationnels et humains nécessaires au bon fonctionnement de la gouvernance et est le garant d’une démarche structurée d’identitovigilance dans la structure.

Le RNIV impose la mise en place d’une instance de gouvernance de l’identitovigilance (RNIV 3, Exi SNH 01). Il n’est pas indispensable de créer une instance dédiée : les missions de gouvernance peuvent être assurées par une instance existante dans la structure (comité de direction, comité qualité, etc.).

|  |
| --- |
| **Extraits du RNVI 3 – V1.2 (20/05/2021)**  *2.2.1.1 Missions*  *L’instance de pilotage cumule les fonctions des instances stratégique et opérationnelle. Elle est chargée, dans le cadre de l’identitovigilance, de :*   * *définir la politique d’identitovigilance et les moyens nécessaires à sa conduite ;* * *réaliser l’analyse des risques a priori (cartographie des risques) ;* * *conduire le plan annuel ou pluriannuel d’actions d’amélioration ;* * *effectuer un suivi des actions et de leurs résultats en s’appuyant sur des indicateurs pertinents ;* * *communiquer sur la politique et ses résultats ;* * *organiser la formation des professionnels, dans le cadre du plan de formation de la structure ;* * *mener des actions de sensibilisation au profit des usagers et des partenaires externes ;* * *formaliser et/ou actualiser les documents qualité relatifs à l’identitovigilance ;* * *mettre en œuvre des retours d’expériences pour les événements indésirables ;* * *réaliser des audits de pratiques ;* * *contrôler la qualité des identités numériques utilisées par la structure et corriger les anomalies (doublons, collisions...) ;* * *participer si nécessaire au rapprochement d’identités entre structures ;* * *effectuer la veille réglementaire et technique...*   *2.2.1.2 Composition*  *La composition de l’instance de pilotage dépend de la taille de la structure qui la porte et de l’organisation mise en œuvre en termes de coordination de la gestion des risques (GDR). Les membres sont désignés par le responsable (ou le coordonnateur) de la structure.*  *La composition recommandée est la suivante, par fonctions (responsable en titre ou représenté) :*   * *le responsable de la structure (ou du groupe) ;* * *le médecin et/ou l’infirmier coordonnateur (ou équivalent) ;* * *le responsable qualité gestion des risques de l’établissement ou équivalent ;* * *le référent en identitovigilance de la structure ;* * *le responsable du système d’information ou équivalent ;* * *des représentants des professionnels de la structure.*   *Dans la mesure du possible, et si cela est pertinent au regard de l’activité de l’établissement ou de son groupe, il peut être associé :*   * *des référents en identitovigilance de structures partenaires (pharmacie, laboratoire, imagerie, établissement de santé... ) ;* * *un représentant des usagers*   *.* |

Le RNIV n’impose pas non plus une organisation particulière de cette instance. En fonction du périmètre d’action des établissements (pôle, site, public accueilli…), une instance de coordination peut compléter le dispositif, notamment pour les sujets mobilisant les ressources transversales (délégué à la protection des données (DPO), responsable de la sécurité des systèmes d'information (RSSI), etc.).

Le principe de fonctionnement de cette instance doit être défini dans un document qui précise :

* La périodicité ;
* La composition ;
* Les thèmes à aborder systématiquement ;
* Les modalités d’enregistrement et de diffusion des décisions.

Il est préconisé de prévoir au moins une réunion trimestrielle pour initialiser efficacement la démarche. La périodicité pourra être révisée selon l’avancée des actions et des résultats obtenus. Les réunions sont planifiées à l’année afin d’assurer la disponibilité des participants et de maintenir la dynamique.

|  |
| --- |
| **Sujets à aborder dans chaque réunion de l’instance de gouvernance** :   * La politique d’identitovigilance (veille réglementaire et ajustement) * Les évènements indésirables (EI) (y compris dysfonctionnements liés au système d’information (SI) et des suites données * L’analyse des indicateurs et les actions d’amélioration à mettre en place si nécessaire * La restitution des principaux résultats des évaluations * Suivi du plan d’action * Adéquation des moyens humains et techniques dévolus à l’identitovigilance et de l’organisation * La gestion documentaire (procédures à rédiger, à actualiser) * Le plan de formation en identitovigilance * Questions diverses (évolution de l’organisation de la structure, remontées terrain…)   Chacun de ses sujets doit être consigné dans le compte-rendu, y compris en l’absence d’actualité. |

L’instance définit les actions à mettre en œuvre et leurs pilotes. Le référent en identitovigilance contrôle et coordonne la mise en œuvre du plan d’action.

Les membres de l’instance de pilotage de l’identitovigilance ne doivent pas hésiter à rechercher des appuis externes, notamment auprès :

* de l’instance opérationnelle régionale d’identitovigilance (si existante, cf. la [liste des référents régionaux](https://esante.gouv.fr/sites/default/files/media_entity/documents/INS_Liste%20des%20referents%20regionaux_Vjuillet_0.pdf) publiée par l’Agence du numérique en santé (ANS) ;
* de la structure régionale d’appui (SRA) à la qualité et à la sécurité des soins (cf. la [liste des SRA](https://www.forap.fr/sra) publiée par la Fédération des organismes régionaux et territoriaux pour l'amélioration des pratiques en santé (FORAP)).

## Le référent en identitovigilance

Le RNIV impose la nomination d’un référent en identitovigilance (RNIV 3 - Exi SNH 02).

Il s’agit d’un professionnel qui pilote la mise en œuvre de l’identitovigilance dans la structure.

La désignation d’un référent est un acte important. Le profil est à déterminer en fonction de l’organisation existante et des missions et moyens qui lui seront confiés. La direction peut s’appuyer sur la fiche repère du référent en identitovigilance en structure médico-sociale[[1]](#footnote-2) et du modèle de fiche de poste[[2]](#footnote-3) proposé dans ce kit pour identifier son référent en identitovigilance.

La légitimité de la fonction est un des facteurs clés de la réussite de la démarche[[3]](#footnote-4).

# Fiche pratique - Identification primaire

L’identification primaire permet d’attribuer une identité numérique unique à un usager dans le système d’information dont la cible est le dossier usager informatisé (DUI)[[4]](#footnote-5). Elle comprend les étapes de recherche, création, modification de l’identité numérique ainsi que l’attribution d’un niveau de confiance à cette identité.

Le respect des bonnes pratiques d’identification primaire est essentiel pour disposer d’une identité numérique unique et fiable de l’usager. Le référentiel national d’identitovigilance (RNIV) décrit de façon détaillée les bonnes pratiques d’identification primaire (cf. RNIV 1, chapitre 3). Seuls les grands principes seront rappelés ci-après.

## Notions clés

**Identité nationale de santé (INS)**

L’INS est une identité numérique provenant de bases nationales d’état civil[[5]](#footnote-6). Elle doit être utilisée depuis le premier janvier 2021 pour référencer, échanger et partager les données de santé[[6]](#footnote-7). L’utilisation de l’INS s’appuie sur un corpus réglementaire important, en particulier sur l’arrêté du 27 mai 2021[[7]](#footnote-8) qui rend opposables : le référentiel INS, le RNIV et le guide d’implémentation de l’INS.

Cette INS est une identité unique, pérenne, partagée par tous les professionnels qui prennent en charge les usagers sur le plan sanitaire et médicosocial. Elle a pour objet d’améliorer la qualité et la sécurité des accompagnements et la coordination des parcours.

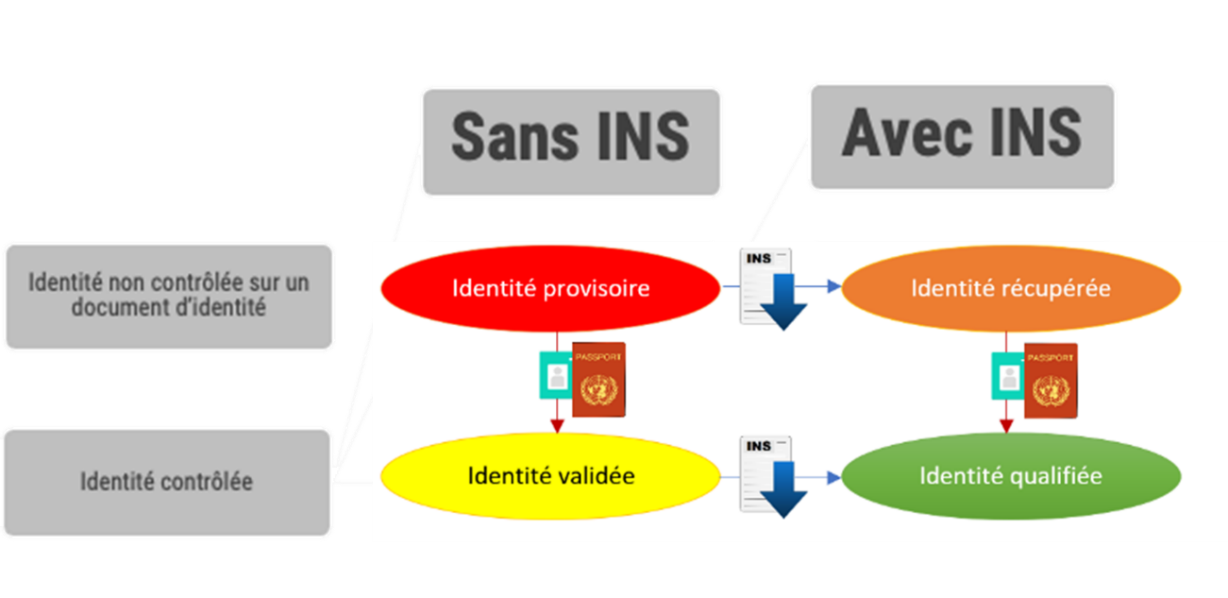
Pour être utilisée en toute sécurité, cette INS doit être *qualifiée*.

**Statuts de l’identité numérique**

Le niveau de confiance d’une identité numérique est défini par 4 statuts :

* *Identité* ***provisoire*** : statut par défaut d’une identité numérique créée localement ;
* *Identité* ***validée*** : statut acquis par une identité numérique créée localement après contrôle de cohérence des traits à partir d’un dispositif à haut niveau de confiance (passeport, carte nationale d’identité, …[[8]](#footnote-9);
* *Identité* ***récupérée*** : statut d’une identité numérique récupérée via le téléservice INSi ;
* *Identité* ***qualifiée*** : statut d’une identité numérique **récupérée** ET **validée.**

L’utilisation des statuts de l’identité numérique est obligatoire (RNIV 1 - Exi PP 07).



**Attributs de l’identité numérique**

Des informations complémentaires peuvent être apportées par l’utilisation d’un attribut.

* *Identité* ***homonyme*** : est utilisée pour signaler des identités à fort taux de ressemblance ;
* *Identité* ***douteuse*** : est utilisée en cas de doute sur l’identité alléguée par l’usager (usager confus, suspicion d’utilisation frauduleuse d’identité, ...) ;
* *Identité* ***fictive***: est utilisée lors de la création volontaire d’une fausse identité (anonymat, …).

L’utilisation des attributs est facultative mais recommandée.

Les attributs *Identité douteuse* et *Identité fictive* ne peuvent être associés qu’au statut *Identité provisoire*, et interdisent l’appel au téléservice INSi. Il n’y a pas de limite aux statuts pouvant être associés aux identités numériques ayant l’attribut *Identité homonyme*.

**Format de saisie de l’identité numérique**

|  |  |
| --- | --- |
| Trait de l’identité numérique | Format de saisie (extrait RNIV1 version 1.2) |
| Date de naissance | JJ/MM/AAAA |
| Nom de naissance | Caractères majuscules  Sans signe diacritique[[9]](#footnote-10) et sans abréviation  Tirets + apostrophes conservés |
| Prénom(s) de naissance |
| Nom utilisé |
| Prénom utilisé |
| Code du lieu naissance | Les 5 caractères numériques du code officiel géographique (COG) de la commune ou du pays de naissance |
| Sexe | M ou F |

|  |  |
| --- | --- |
| Une image contenant texte, gants  Description générée automatiquement[[10]](#footnote-11) | Pour créer une identité numérique, il est obligatoire de renseigner au moins 5 traits :   * Date de naissance * Nom de naissance * 1er Prénom de naissance * Code du lieu naissance * Sexe |

## Bonnes pratiques organisationnelles

Il est indispensable de limiter le nombre de personnes et de lieux où les identités numériques peuvent être créées. Dans la mesure du possible les créations d’identités doivent être limitées à des professionnels spécifiquement formés.

L’attribution des droits de gestion de l’identité numérique[[11]](#footnote-12) dans le DUI doit être maitrisée, formalisée et contrôlée :

* Les droits de modification d’identité, y compris par appel au téléservice INSi, doivent être limités au personnel en charge de l’identification primaire ;
* La recherche et le traitement des anomalies (doublons, collisions) sont des opérations sensibles qui ne doivent être réalisées que par un nombre restreint de professionnels spécifiquement formés (dont le référent en identitovigilance).

## Bonnes pratiques de la création d’une identité numérique

* Afin de sécuriser le recueil de l’identité, l’usager (ou son accompagnant), doit être interrogé :
  + En utilisant des questions ouvertes, y compris en présence d’une pièce d’identité, de type :
    - * Quel est votre nom de naissance ?
      * Quel est votre prénom ?
      * Quelle est votre date de naissance ?...
  + En lui demandant d’épeler les noms et prénoms si besoin,
  + En faisant préciser la présence ou l’absence de tiret séparant les deux parties du nom ou du prénom,
  + En levant le doute lorsque nom et prénom peuvent être confondus (exemple : PIERRE MARTIN) ;
* La création d’une identité numérique doit toujours être précédée par une étape de recherche dans la base locale des identités numériques de la structure, encore appelée *référentiel d’identités*. Cette recherche peut être rendue obligatoire par certains logiciels.
  + Les règles de recherche d’une identité numérique doivent être connues et respectées par les professionnels et les éditeurs de logiciel, en cohérence avec les modalités décrites dans le RNIV 1 (Exi SI 01, Exi SI 02 et Reco PP 01) et le Guide d’implémentation de l’INS.
  + Il faut utiliser la date de naissance comme premier critère et compléter éventuellement par le début du nom de naissance ou du prénom.
  + Les règles de saisies définies dans le RNIV (Annexe IV RNIV 1) doivent être connues et appliquées par l’ensemble des acteurs habilités à créer ou modifier une identité numérique.
* Si l’établissement réalise l’enregistrement de l’identité numérique en leur présence, il est conseillé de demander à l‘usager ou à son accompagnant de vérifier les traits saisis (sur un écran, une fiche imprimée...) avant de procéder à la validation.
* La conservation d’une copie de pièce d’identité nécessite le respect de conditions de sécurité mentionnées dans la fiche pratique FIP 06 "Gestion des copies de pièces d’identité dans le système d’information” publiée par le Réseau des référents régionaux en identitovigilance (3RIV)[[12]](#footnote-13).
* Des procédures spécifiques doivent être formalisées pour préciser la conduite à tenir dans des cas particuliers ; le Réseau des référents régionaux en identitovigilance (3RIV) propose des fiches pratiques (FIP) dédiées[[13]](#footnote-14) :
  + La gestion des identités particulières comme l’anonymat (cf. FIP 03[[14]](#footnote-15) et FIP 04[[15]](#footnote-16)) ;
  + La gestion des erreurs dans la base identité (doublons, collisions, …) ;
  + La suspicion d’utilisation frauduleuse d’une identité (cf. FIP 05[[16]](#footnote-17)) ;
  + La discordance entre l’identité locale et l’INS (cf. FIP 07[[17]](#footnote-18)).

|  |
| --- |
| **Synthèse de la fiche pratique FIP 06 - Gestion des copies de pièces d’identité dans le système d’information, publiée par le réseau des Référents régionaux en identitovigilance (3RIV)**  La conservation des copies des pièces et saisie des numéros.  La Commission Nationale de l'Informatique et des Libertés (CNIL) a compris les enjeux de sécurité liés à la vérification d’une identité qui peut parfois être nécessaire à distance de la venue d’un usager.  Après une saisine de la direction interministérielle du numérique en santé (N° 20017187), elle a rendu un avis, en date du 5 novembre 2020 (non publié à ce jour), autorisant les établissements à conserver durant 5 ans après la dernière venue de l’usager une copie d’une pièce d’identité.  Dans cet avis, la CNIL précise que :   * L’usager doit être informé de cette conservation et de ses objectifs ; * Les informations sur la nature de la pièce peuvent être enregistrées, à l’exception du numéro du titre d’identité ; * Les copies de pièces d’identité doivent être conservées dans des conditions assurant un cadre protecteur pour les droits et les libertés des personnes ; elles comprennent :   + Le chiffrement des pièces d’identité,   + La limitation de l’accès à cette copie aux professionnels spécifiquement habilités en charge du traitement des anomalies liées à l’identité,   + La traçabilité et l’historisation des consultations ; * Les établissements doivent disposer d’une procédure garantissant la destruction des copies numériques et papier au-delà du délai de 5 ans après la dernière venue de l’usager ; * Les pièces d’identité échangées entre cellules d’identitovigilance locales territoriales ou régionales doivent l’être en utilisant des dispositifs sécurisés ; * Les critères permettant d’évaluer la justification de demandes de communication des pièces d’identité doivent être définies. |

# Fiche pratique - Identification secondaire

L’identification secondaire est à mettre en œuvre par toutes les personnes appelées à accompagner ou soigner l’usager, après que son identité numérique a été définie. Elle a pour objet de garantir que les prestations sont délivrées au bon usager et que les informations sont enregistrées dans le bon dossier. Elle consiste à intégrer des barrières de sécurité, dans les pratiques quotidiennes, afin de s’assurer que l’identité numérique enregistrée sur les documents et outils utilisés pour la prise en charge de l’usager (écran Dossier Usager Informatisé (DUI), prescription, étiquette d’identification, pilulier, plateau repas, etc.) correspondent à l’identité physique de l’individu.

## Pourquoi est-ce nécessaire ?

Les erreurs d’identification secondaire sont à l’origine des événements indésirables les plus fréquents : interversion des traitements entre deux usagers, renseignement des données d’un usager dans le dossier d’un autre ouvert dans le DUI, envoi à un professionnel d’un document qui n’est pas celui attendu…

Les problématiques d’identification secondaire sont majoritairement liées à la méconnaissance des usagers par les professionnels : intérimaire, vacataire, étudiant, nouveau salarié…

Les erreurs peuvent également être liées à :

* Un défaut d’attention (routine, interruption de tâche, …) ;
* La méconnaissance des règles de sécurité ;
* Des pratiques de communication associées à un lieu de vie (par exemple : l’utilisation d’un surnom non officiel, d’un signe pour un usager malentendant, …).

## Les bonnes pratiques à mettre en œuvre

Les bonnes pratiques d’identification secondaire sont basées sur un certain nombre de principes qui doivent être appliqués en routine. La vérification de l’identité de l’usager pris en charge doit être réalisée selon la capacité de celui-ci à participer à son identification et selon la connaissance de l’usager par le professionnel.

Au regard de la diversité des établissements, des modes de prise en charge et du public accueilli, il n’est pas possible de faire des recommandations standards pour l’identification secondaire. Les équipes doivent analyser les cas d’usage pour adapter les pratiques et sécuriser l’identification.

Le personnel doit s’interroger sur l’identité de l’usager en mobilisant les mécanismes possibles :

* Photographie[[18]](#footnote-19) (par exemple : sur le pilulier, la porte de chambre, trombinoscope, …)
* Questions ouvertes (nom de naissance, premier prénom de naissance, date de naissance)
* Dispositifs physiques d’identification occasionnels ou permanents : badge d’identification, bracelet…

|  |
| --- |
| **Préconisations**  Ces mécanismes d’identification sont à adapter en fonction des capacités des usagers et des types d’établissements afin de garder un équilibre entre le confort de vie, le respect de la personne et les impératifs de sécurité.  Une réflexion éthique sur ce sujet peut être conduite avec le conseil de la vie sociale (CVS). |

Autres recommandations :

* La formation aux bonnes pratiques d’identification secondaires doit être régulièrement réalisée et évaluée ;
* Des actions particulières doivent être proposées au personnel non permanent afin de sécuriser l’identification secondaire (par exemple : livret d’accueil, tutorat, …) ;
* Dans le cadre d’un transport exceptionnel et non accompagné, un dispositif physique d’identification doit être utilisé ;
* Les photographies[[19]](#footnote-20) doivent être renouvelées régulièrement autant pour les adultes que pour les enfants, tous les 6 mois par exemple ;
* Les photographies des usagers sont à intégrer dans le DUI ;
* L’identification secondaire doit être favorisée par un affichage adéquat de l’identité sur les différents écrans du DUI et sur les différents documents utilisés pour accompagner l’usager.

# Fiche pratique – Pilotage du déploiement de l’identitovigilance et de la démarche d’amélioration

## Sur quelles données s’appuyer ?

Le pilotage de la démarche d’amélioration continue des pratiques dans le domaine de l’identitovigilance nécessite de pouvoir s’appuyer sur des données objectives et mesurables. C’est le rôle des indicateurs.

Habituellement exprimés sous forme d'un taux, ils permettent d'objectiver la situation avant et après la mise en œuvre d'une action. Instruments de pilotage et d’aide à la décision, l’indicateur isolé comme le tableau de bord des indicateurs peuvent aussi servir à :

* Communiquer les résultats obtenus (rapport d'activité) ;
* Faciliter la comparaison des résultats avec ceux, de nature identique, déclarés par d'autres organisations comparables (parangonnage).

On peut définir un indicateur pour évaluer différentes situations comme :

* La cohérence des moyens (exemple : *taux d’applications de santé utilisées dans la structure en capacité de gérer l’Identité Nationale de Santé (INS)*) ;
* L'efficacité et la conformité d'un processus (exemple : *taux de doublons générés par chacun des services assurant l'accueil des usagers*) ;
* Les résultats d'actions d'amélioration (exemple : *taux de professionnels de la structure ayant bénéficié d'une formation à l’identitovigilance depuis moins de 3 ans*).

La mise en place d'un indicateur nécessite de respecter plusieurs critères afin de s’assurer qu’il reflètera bien les résultats de ce qu'il est censé mesurer (*spécificité*) mais pas davantage (*biais*). Il est idéalement présenté sous la forme d’une *fiche descriptive*, également appelée *carte d’identité de l’indicateur.* Celle-ci doit détailler notamment :

* La finalité de l'indicateur ;
* Ses modalités pratiques de calcul ;
* Les seuils de performance (minimum acceptable, objectif visé) ;
* Les conditions et les biais potentiels d’interprétation de la donnée.

Il est préconisé que les indicateurs relatifs à une même thématique soient réunis dans un seul document ou écran d'affichage, appelé *tableau de bord des indicateurs*. Il permet d'améliorer la pertinence de leur analyse et des actions correctives à mettre en œuvre si les résultats ne correspondent pas aux attentes. Comme les indicateurs qu’il regroupe, un tableau de bord doit également respecter un certain nombre de critères :

* Comporter un nombre limité d’indicateurs ;
* Se limiter à ceux qui concernent la thématique évaluée ;
* Offrir une vue d’ensemble des résultats ;
* Être facile à actualiser ou à faire évoluer en fonction des besoins.

## Quels indicateurs doit-on suivre ?

Le référentiel national d’identitovigilance (RNIV) donne un certain nombre d’exemples d'indicateurs à suivre en termes d’identification primaire et de gestion des risques (cf. § 2.5 RNIV 3).

En identification primaire, il est important d’évaluer la qualité du référentiel d’identités et l’efficacité du traitement des anomalies. Les indicateurs les plus fréquemment utilisés sont :

* Taux d’identités numériques au statut *identité validée* ;
* Taux d’identités numériques au statut *identité qualifiée* ;
* Taux de doublons dépistés dans la file active des usagers accompagnés;
* Nombre ou taux de collisions détectées;
* Nombre ou taux d’évènements indésirables (EI) relatifs à l’identification primaire.

En identification secondaire, il est nécessaire de suivre le respect des bonnes pratiques d’identification par les professionnels. Les indicateurs les plus fréquemment utilisés sont :

* Taux des évènements porteurs de risques (EPR)[[20]](#footnote-21) ou presque accident relatifs à l’identification secondaire ;
* Taux des évènements indésirables relatifs à l’identification secondaire.

La formation des professionnels est suivie par des indicateurs *ad hoc* évaluant les taux de professionnels formés en distinguant ceux qui ont la charge de l’identification primaire de ceux qui accompagnent les usagers et donc plutôt concernés par l’identification secondaire. Il est intéressant aussi de distinguer la part des nouveaux arrivants et des professionnels intérimaires ayant bénéficié d’une formation à leur arrivée.

Il est conseillé de s’approprier les indicateurs proposés par le Réseau des référents régionaux en identitovigilance (3RIV) : cf. documents IND 01 à IND 05 dans les [documents publiés par cette association](https://resana.numerique.gouv.fr/public/information/consulterAccessUrl?cle_url=2146736381BW9TM1VZCDQAbQhuBWsAIAc5WmcGJwZvAmlQbQdmXW5TaAM/UjkAYlRu).

Par ailleurs, les instances régionales ou nationales peuvent décider de rendre obligatoires le recueil et la transmission de certains d’entre eux. Elles sont également en capacité d’en fournir (exemple : *indicateur de déploiement du téléservice INSi par département, éditeur et structure* fourni par le [GIE SESAM Vitale](https://www.sesam-vitale.fr/insi)).

## Recueillir et analyser les indicateurs

La construction, le recueil et l’interprétation des indicateurs sont à réaliser sous l’autorité de l’instance de gouvernance ou de coordination (cf. fiche pratique Gouvernance du présent document).

Une périodicité de mesure et d’analyse, de préférence trimestrielle, permet de piloter finement la thématique et de mettre en place rapidement des actions correctives si nécessaire.

# Fiche pratique - Gestion des risques

## Notion de gestion des risques

La gestion des risques (GDR) fait partie de la démarche d’amélioration continue de la qualité. Elle a pour objet de lutter contre les événements indésirables (EI). On peut distinguer deux étapes :

* la GDR *a priori* qui consiste à identifier les situations à risque d’erreur d'identification et de les lister (cartographie des risques) afin d’en prévenir la survenue par la mise en place des barrières de sécurité (adaptation des pratiques, formation, information, sensibilisation, contrôle...) ;
* la GDR *a posteriori* qui, comme son nom l'indique, se met en place après la survenue d’un EI. Son efficacité repose sur un certain nombre de facteurs comme :
  + la culture de sécurité des professionnels de la structure et notamment leur adhésion au signalement des EI[[21]](#footnote-22),
  + la réalisation de retours d’expériences (REX) qui consistent à analyser le déroulement de l’EI, d’identifier les facteurs qui ont permis sa survenue et de déterminer les actions correctives et/ou préventives à mettre en œuvre pour en éviter la récidive ou limiter ses effets,
  + la mise en œuvre effective des actions d’amélioration,
  + le partage d'expériences (avec les autres professionnels et structures afin qu’ils puissent apprendre à leur tour des erreurs des autres et mettre en œuvre les actions préventives qui s’imposent).

## Identification des événements indésirables en identitovigilance

Tout ce qui entraîne une erreur d’identification est qualifié d’EI en identitovigilance. Il est important d’identifier les situations porteuses d’EI afin de déterminer les barrières de sécurité à mettre en place pour les prévenir ou en limiter les conséquences.

Il est utile de faire la distinction entre les EI liés à des problèmes d’identification primaire et ceux qui sont associés à des mauvaises pratiques d’identification secondaire. Les acteurs concernés étant différents, les actions correctrices le seront aussi.

**Dans le cadre de la GDR *a priori***, il faut intégrer les EI en identitovigilance dans la cartographie des risques identifiés par la structure. Il convient de s’interroger collectivement sur les situations susceptibles d’entraîner une erreur d’identification dans le cadre des processus de l’établissement : premier contact, création ou modification de l’identité numérique, récupération de l’Identité Nationale de Santé (INS), prise en charge de l’usager, distribution de repas ou de médicaments, impression d’étiquettes, transmission de données de santé, etc.

Pour chaque situation identifiée, il faut évaluer :

* les impacts potentiels de l’erreur en calculant sa « criticité » (probabilité de survenue x dangerosité),
* l’existence et la robustesse des barrières existantes (procédures de bonnes pratiques),
* la possibilité de mettre en place des barrières de sécurité plus opérationnelles.

**Dans le cadre de la GDR *a posteriori***, il faut déclarer (signaler) tous les dysfonctionnements en relation avec l’identification des usagers : ceux qui ont eu des conséquences sur l’organisation ou la qualité de la prise en charge mais également les événements qui ont été corrigés juste à temps ; ces derniers sont appelés « presque-accidents » ou « événements porteurs de risque » (EPR).

Le signalement doit utiliser de préférence le système de signalement interne des EI de la structure (sous forme papier ou informatique), à condition que les critères de déclaration des EI en identitovigilance soient bien prévus. Il peut être aussi envisagé l’utilisation d’un formulaire spécifique de déclaration des EI en identitovigilance[[22]](#footnote-23).

|  |
| --- |
| **Signalement des événements indésirables**  Le signalement des EI est au cœur de la culture de sécurité des professionnels et de la démarche d’amélioration continue de la qualité. Il faut signaler les EI qui sont à l’origine d’effets néfastes avérés (sur un usager, sur le fonctionnement de la structure) mais également les erreurs, *a priori* sans conséquences, mais qui auraient pu en avoir.  La déclaration d’une erreur relative à l’identification d’un usager n’est pas spécifique. Elle doit suivre le circuit habituel de signalement interne à la structure, précisé dans une procédure *ad hoc*.  Le signalement doit être effectué le plus rapidement possible après la survenue de l’EI. Cela permet de prendre les mesures appropriées en interne.  Le système de gestion des signalements doit permettre de classer chaque EI selon sa typologie principale (par exemple : système d’information, identification, médicament, transport…).  **Charte de confiance**  Pour que le signalement des EI fasse partie de la culture de sécurité des professionnels, il est particulièrement important que cette démarche soit réalisée dans un climat de confiance où le déclarant ne court pas le risque d’être culpabilisé par ses collègues ou sa direction. Chaque structure devrait disposer d’une charte de confiance ou charte d’incitation au signalement, signée par la direction . Ce dispositif garantit l’objectivité et la transparence nécessaire à cet exercice. |

Le recours à des REX a notamment pour objectif de rechercher les barrières qui n’ont pas fonctionné et d’imaginer de nouvelles parades pour éviter une récidive.

## Typologie des EI relatifs à l'identitovigilance

L’événement indésirable en identitovigilance peut être associé :

* Dans le cadre de l’identification primaire, à l’attribution d’une identité numérique erronée à l’usager :
  + erreur de saisie des traits d’identité,
  + mauvaises pratiques de recherche d’antériorité,
  + anomalie de sélection d’un usager dans la base de données ;
* Dans le cadre de l’identification secondaire(source la plus fréquente des EI en identitovigilance) à l’erreur :
  + de l’usager à qui on propose un accompagnement ou chez qui on réalise un soin,
  + de dossier dans lequel on consulte ou on enregistre les données relatives à la prise en charge,
  + d’étiquetage d’un échantillon, d’un document,
  + de rangement ou d’envoi de données de santé...

## GDR au niveau régional

La réglementation impose le signalement de certains EI aux autorités sanitaires et notamment aux Agences régionales de santé (ARS)[[23]](#footnote-24). C’est le cas notamment :

* d’un d’événement indésirable grave associée au soins (EIGS)[[24]](#footnote-25) qui est conjoint à un préjudice grave (décès, mise en jeu des fonctions vitales, séquelles définitives). Il fait l’objet d’une procédure de signalement spécifique sur le portail de signalement national des événements sanitaires indésirables[[25]](#footnote-26),
* d’un EI associé à une vigilance réglementaire[[26]](#footnote-27) comme la pharmacovigilance (effet néfaste d’un traitement médicamenteux lié ou non à une erreur) qui peut également être déclaré sur le portail national de signalement,
* des accidents ou incidents liés à une erreur ou à un défaut de soin ou de surveillance[[27]](#footnote-28).

Pour le signalement et la gestion des EI, les structures médicosociales peuvent solliciter :

* la *structure régionale d’appui à la qualité et à la sécurité* (SRA) pour la mise en œuvre de la démarche qualité,
* l*’instance régionale opérationnelle d’identitovigilance*, lorsqu’elle existe, pour accompagner les actions d’amélioration spécifiques à l’identification[[28]](#footnote-29),
* la *plateforme régionale de veille et d’urgence sanitaire* de leur ARS pour les modalités de signalement et de prise en charge de l’EI.

## Références utiles

* Document « [MEM 01 - Signalement et gestion des événements indésirables relatifs à l’identification des usagers](https://resana.numerique.gouv.fr/public/information/consulterAccessUrl?cle_url=2111870202UDoObgYKCDRSPwVjAW9QcAc5DjMGJwNqAGtWawRlWmkDNwQ4WjxTM1xv) » publié par le Réseau des référents régionaux en identitovigilance (3RIV).
* Guide "[Analyse des événements indésirables associés aux soins](https://www.has-sante.fr/upload/docs/application/pdf/2021-09/guide_lanalyse_des_evenements_indesirables_associes_aux_soins_eias.pdf)" réalisé conjointement par la Haute autorité de santé (HAS) et la fédération des structures régionales d’appui (FORAP).
* Documents d’aide de la série "[Comprendre, signaler, gérer](https://www.rreva-na.fr/travaux/comprendre-signaler-gerer)" éditée par le Réseau régional de vigilances et d'appui de Nouvelle-Aquitaine (RREVA-NA)
* Exemples de gestion d’EI en identitovigilance comme les [*Fiches de partage d'expérience*](https://www.identito-na.fr/actions-communication#partage) éditées par la Cellule régionale d’identitovigilance de Nouvelle-Aquitaine

# Fiche pratique – Matrice RACI mise en œuvre de l’Identitovigilance dans le secteur médico-social

*Il est à noter que la matrice RACI constitue une proposition et sera à adapter aux organisations des établissements et services. Un modèle modifiable est à votre disposition (outils du présent kit).*

Légende : **A : Autorité** = responsable de la décision (il ne devrait n’y avoir qu’un A par ligne) ; **R : Réalisateur** = acteur(s) impliqué(s) dans la mise en œuvre de l’action ; **C : Consulté** = partie(s) dont l’avis doit être pris en compte avant d’arrêter une action ; **I : Informé** = partie(s) dont l’information est utile.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thème** | **Actions à conduire** | **Dir.1** | **Réf. IV** | **Resp. qualité** | **RH** | **Resp. soins/**  **Accompagnement2** | **Resp.**  **admission 3** | **Resp. SI4** | **DPO** |
| **Gouvernance** | S'assurer de l'existence d'une instance stratégique, de niveau établissement ou groupe, pilotant ou en capacité de piloter les actions à conduire dans le cadre du déploiement de l'INS et des bonnes pratiques en identitovigilance. La mettre en place si ce n’est pas le cas. | AR | C | C | C | C | C | C | I |
| Désigner officiellement le(s) référent(s) en identitovigilance de niveau établissement, groupe d’établissements ou organisme gestionnaire. | AR |  | C | R | C | C | C | I |
| Vérifier l'adéquation de l’organisation aux besoins d'accompagnement des acteurs (formation, sensibilisation, gestion des risques, évaluation des pratiques...). | AR | R | R | R | C | C | C | I |
| Evaluer l'intérêt de mettre en place des correspondants en identitovigilance sur sites pour relayer l’action du référent. | C | AR | C | R | C | C | I | I |
| Définir les outils de pilotage (indicateurs et modalités de suivi) | AR | R | C | I | C | C | C | I |
| **Système d’information** | Vérifier la compatibilité du DUI au Guide d’implémentation de l’INS et au RNIV. | A | R | I | I | I | I | R | C |
| Vérifier la capacité du DUI à interroger le téléservice INSi. | I | C | I | I | I | C | AR | I |
| Piloter l’implémentation technique de l’interrogation du téléservice INSi | I | C | I | I | C | C | AR | C |
| Identifier les flux à mettre en œuvre avec les partenaires professionnels et applications d’e-santé. | I | C | I | I | C | I | AR | C |
| **Bonnes pratiques en matière d’identification et gestion des risques** | Mettre en place une organisation pour assurer l’identification primaire (recherche, création, modification de l’identité numérique) selon les principes du RNIV. | A | R | R | R | C | R | C | I |
| Mettre en œuvre la gestion des risques liés à l’identification en termes de gestion des risques à priori et à postériori. | C | R | AR | I | R | R | R | R |
| Assurer l’évaluation des pratiques d’identification. | I | R | AR | I | R | R | I | I |
| **Documentation** | Constituer un corpus documentaire en identitovigilance conforme aux règles de bonne pratique du RNIV | I | R | AR | I | R | R | R | I |
| Formaliser et communiquer la charte d’identitovigilance. | AR | R | R | R | R | R | R | R |
| Définir les procédures opérationnelles à formaliser. | I | R | R | I | R | R | R | C |
| Réviser ou rédiger la charte d’utilisation du système d’information en intégrant les principes d’identitovigilance. | C | R | C | I | C | C | AR | C |
| Réaliser une cartographie des flux applicatifs. | I | I | I | I | I | I | AR | I |
| Définir et mettre à jour les habilitations, droits d’accès, de création, modification et gestion avancée des identités numériques. | A | R | C | R | C | C | R | C |
| **Sensibilisation et formation** | Identifier l’ensemble des acteurs concernés et leurs besoins en termes de formation ou de sensibilisation | A | R | C | R | R | R | C | I |
| Mettre en place un programme de formation adapté et gradué. | C | C | C | AR | C | C | C | I |
| Réaliser un bilan des formations. | I | R | R | AR | I | I | I | I |

1 : selon la taille et l’organisation de la structure, ce peut être la direction d’établissement et/ou direction générale.

2 : personne en charge de la coordination globale des soins ou de l’accompagnement sur l’établissement. Pour les établissements ‘médicalisés’, cadre de santé ou médecin coordinateur s’il existe. Pour les établissements non médicalisé, directeur ou chef de service.

3 : Personne en charge de l’enregistrement de l’identité des usagers dans le DUI (chef de service, assistante de direction, secrétaire médicale, secrétaire administrative…).

4 : personne en charge des systèmes d’informations.

# Glossaire et définitions

|  |  |
| --- | --- |
| 3RIV : | Réseau des référents régionaux en identitovigilance |
| ANS : | Agence du numérique en santé |
| ARS : | Agence régionale de santé |
| CNIL : | Commission Nationale de l'Informatique et des Libertés |
| CVS : | Conseil de la Vie Sociale |
| DPO : | Délégué à la protection des données (ou DPD) |
| DUI : | Dossier usager Informatisé |
| EI : | Evénement indésirable |
| EIGS : | Evénement Indésirable grave associé aux soins |
| EPR : | Evénement Porteur de Risques |
| FORAP : | Fédération des organismes régionaux et territoriaux pour l'amélioration des pratiques en santé |
| GDR : | Gestion des risques |
| INS : | Identité nationale de santé |
| REX : | Retours d’EXpériences |
| RNIV : | Référentiel national d’Identitovigilance |
| RSSI : | Responsable de la sécurité des systèmes d'information |
| SI : | Système d'information |
| SRA : | Structure Régionale d'Appui à la qualité des soins et à la sécurité des patients |

|  |  |
| --- | --- |
| Identification primaire | Phase de l'identification de l'usager qui a pour objet de lui attribuer une identité numérique ou de la corriger. Elle comprend les actions réalisées pour rechercher une identité numérique préalablement enregistrée dans le système d'information (DUI) de la structure, la créer ou la modifier y compris en termes de statut et d'attributs associés à cette identité numérique |
| Identification secondaire | Pratiques d'identification à mettre en œuvre par chaque professionnel appelé à accompagner ou soigner un usager, afin de s'assurer de prendre en charge la bonne personne et d'utiliser les bons outils pour consulter ou enregistrer les données qui la concernent (écran DUI, prescription, étiquette d’identification, pilulier, plateau repas, etc.). |
| Données de santé | Ce terme regroupe toutes les informations à caractère personnel susceptibles de révéler directement ou indirectement des informations sur l’état de santé d'un usager. Cette définition englobe donc les données directement relatives à sa maladie, son handicap (antécédents, traitement, résultats d'examens, taux d'invalidité...) ainsi que les informations relatives à une prise en charge sanitaire ou médicosociale (identité numérique, lieu de prise en charge...). |
| Mon espace santé | Mon espace santé est un service qui permet à chaque usager disposant d'une INS de stocker et partager ses documents et données de santé. Il donne accès au dossier médical partagé (DMP), à la messagerie sécurisée de santé citoyenne et à un agenda de santé. Il s'enrichira progressivement d'autres outils numériques compatibles. |
| Téléservice INSi | Le téléservice INSi, mis en œuvre par l'Assurance maladie, sert à effectuer les opérations de récupération et de vérification de l'INS. Il ne peut être appelé que par l'intermédiaire d'un système d'information de santé ayant reçu un agrément CNDA et par un opérateur disposant d'outils d'habilitation adéquat (carte CPx et/ou certificat serveur). |
| Identité provisoire | Statut par défaut d’une identité numérique créée localement avant d'avoir pu effectuer un contrôle ou accéder au téléservice INSi. |
| Identité validée | Statut attribué à une identité numérique créée localement après avoir effectué un contrôle de cohérence des traits d'identification à partir d’un dispositif à haut niveau de confiance (passeport, carte nationale d’identité…). |
| Identité récupérée | Statut d’une identité numérique composée des traits de l'INS récupérés ou contrôlés via le téléservice INSi. |
| Identité qualifiée | Statut d’une identité numérique basée sur l'INS et dont les traits ont été validés lors d'un contrôle de cohérence à partir d’un dispositif à haut niveau de confiance (Identité validée + identité récupérée). |
| Identité homonyme | Attribut pouvant être utilisé pour alerter les professionnels sur le fort taux de ressemblance de l'identité numérique affichée avec une ou plusieurs autres plusieurs identités numériques enregistrées dans le système d'information de la structure. |
| Identité douteuse | Attribut à utiliser pour signaler l'existence d'un doute sur l’identité alléguée par l’usager (usager confus, suspicion d’utilisation frauduleuse de l'identité d'un autre usager...). Il est obligatoirement associé à un statut d'Identité provisoire et interdit l'appel au téléservice INSi. |
| Identité fictive | Attribut pouvant être utilisé pour signaler que l'identité numérique a été volontairement créée sur la base de traits fictifs dans le cas d'une prise en charge anonyme. |
| EPR | Les EPR sont des événements indésirables qui n'ont pas causé de dommage grave au patient. Les termes couramment utilisés pour décrire les EPR sont, par exemple, les dysfonctionnements, les incidents, les précurseurs et les presque accidents. |

# Contenu du kit de déploiement de l’identitovigilance en médicosocial :

**Volet à destination du directeur**

**Volet à destination du référent**

**Volet à destination du DSI**

**Volet à destination du référent qualité et gestion des risques**

**Fiches pratiques :**

* Gouvernance
* Identification primaire et INS
* Identification secondaire
* Pilotage
* Gestion des risques
* Matrice RACI

**Récapitulatif des exigences et recommandations du RNIV**

**Ressources documentaires**

**Comprendre**

1. <https://www.identito-na.fr/sites/default/files/public/2021-09/Fiche_repere_ref_identito.pdf> [↑](#footnote-ref-2)
2. Cf. Fiche de poste Référent en identitovigilance – Outils [↑](#footnote-ref-3)
3. Cf. Volet à destination de la Direction – document IV [↑](#footnote-ref-4)
4. Cartographie fonctionnelle du système d’information médico-social : <https://ressources.anap.fr/numerique/publication/2604> [↑](#footnote-ref-5)
5. Répertoire national d’identification des personnes physiques (RNIPP) pour les usagers nés en France ou Système national de gestion des identifiants (SNGI) pour les usagers nés à l’étranger et couverts par l’Assurance Maladie. Les deux bases RNIPP et SNGI sont synchronisées. [↑](#footnote-ref-6)
6. 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 : <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039196419/> [↑](#footnote-ref-7)
7. Arrêté du 27 mai 2021 paru le 8 juin 2021 portant approbation des modifications apportées au référentiel « Identifiant national de santé » : <https://www.legifrance.gouv.fr/download/pdf?id=GDOgfHYG0QmC-vhiEpj0syfJvp_yqT8SIiOnWW6Q0Fc=> [↑](#footnote-ref-8)
8. Mais aussi le titre de séjour, le livret de famille ou un extrait d’acte de naissance pour les enfants (accompagné d’un titre de haut niveau de confiance d’un parent) [↑](#footnote-ref-9)
9. Un diacritique ou signe diacritique est un élément adjoint à une lettre d'un alphabet pour en modifier la valeur ou pour distinguer des mots homographes. Exemples : accents, cédille, … [↑](#footnote-ref-10)
10. Source : <https://www.hauts-de-france.ars.sante.fr/media/78509/download> [↑](#footnote-ref-11)
11. PGSSI-S – Guide gestion des habilitations d’accès au SI : <https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi-s_guide-gestion-des-habilitations-1.0.pdf> [↑](#footnote-ref-12)
12. [FIP 06\_Gestion des copies de pièces d’identité](https://solidarites-sante.gouv.fr/IMG/pdf/fip_06_gestion_copie_piece_identite_v1_vdgos.pdf) [↑](#footnote-ref-13)
13. [Liste des documents en vigueur publiés par le 3RIV (numerique.gouv.fr)](https://resana.numerique.gouv.fr/public/information/consulterAccessUrl?cle_url=2146736381BW9TM1VZCDQAbQhuBWsAIAc5WmcGJwZvAmlQbQdmXW5TaAM/UjkAYlRu)  [↑](#footnote-ref-14)
14. [FIP 03\_Gestion de la confidentialité et de l’anonymat](https://resana.numerique.gouv.fr/public/information/consulterAccessUrl?cle_url=1058592048AmgHZ1NfADwHagNlVTsDI1BuDjNSc1M6DWYDPgBhDj0IMwA0UjgAY1Bg) [↑](#footnote-ref-15)
15. [FIP 04\_Recommandations bonnes pratiques gestion des identités accouchement dans le secret](https://resana.numerique.gouv.fr/public/information/consulterAccessUrl?cle_url=1111814803Vz0CYgYKU29dMARiAG5ScgA+ATxXdgduAGsFOARlDT4HPFVgVjVUMQM0) [↑](#footnote-ref-16)
16. [FIP 05\_Conduite à tenir utilisation d'une identité frauduleuse](https://resana.numerique.gouv.fr/public/information/consulterAccessUrl?cle_url=1964510906BmwDY1RYAT0BbAlvAmwDIwA+ATwAIQJrDGdQbQRlDj0GMlBsB2EBYQY2) [↑](#footnote-ref-17)
17. [FIP 07\_Conduite à tenir discordance identités numérique et physique de l'usager](https://resana.numerique.gouv.fr/public/information/consulterAccessUrl?cle_url=1838992936VD5XNwMPBDhXOlcxAG5WdlNtDjMEJQZvDWYDPgZnWGsFPwYwUzBVOAY2) [↑](#footnote-ref-18)
18. La diffusion d’une photographie de l’usager est soumise au consentement de l’usager et au droit à l’image [↑](#footnote-ref-19)
19. La diffusion d’une photographie de l’usager est soumise au consentement de l’usager et au droit à l’image [↑](#footnote-ref-20)
20. Les EPR sont des événements indésirables qui n'ont pas causé de dommage grave au patient. Les termes couramment utilisés pour décrire les EPR sont, par exemple, les dysfonctionnements, les incidents, les précurseurs et les presque accidents. [↑](#footnote-ref-21)
21. Cf. Signalement des EI en identitovigilance – outils [↑](#footnote-ref-22)
22. Cf. fiche Signalement des EI liés à l’identification – outils [↑](#footnote-ref-23)
23. Décret N° 2016-1813 du 21 décembre 2016 relatif à l’obligation de signalement des structures médico-sociales

    Décret N° 2016-1606 du 25 novembre 2016 relatif à la déclaration des évènements indésirables graves associés à des soins et aux structures régionales d’appui à la qualité des soins et à la sécurité des patients

    Décret n° 2016-1151 du 24 août 2016 relatif au portail de signalement des événements sanitaires indésirables

    Arrêté du 28 décembre 2016 relatif à l’obligation de signalement des structures sociales et médico-sociales

    Instruction N° DGS/PP1/DGOS/PF2/DGCS/2A/2017/58 du 17 février 2017 relative à la mise en œuvre du décret n° 2016-1606 du 25 novembre 2016 relatif à la déclaration des évènements indésirables graves associés à des soins et aux structures régionales d’appui à la qualité des soins et à la sécurité des patients [↑](#footnote-ref-24)
24. Articles L.1413-14 et R.1416-67 & suiv. du Code de la santé publique [↑](#footnote-ref-25)
25. [Portail de signalement des événements sanitaires indésirables (social-sante.gouv.fr)](https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil) [↑](#footnote-ref-26)
26. Article L.1413- 14 du Code de la santé publique [↑](#footnote-ref-27)
27. Article L.331-8-1 CASF [décret n° 2016-1813 du 21/12/16 et arrêté du 28 /12/16] [↑](#footnote-ref-28)
28. <https://esante.gouv.fr/sites/default/files/media_entity/documents/INS_Liste%20des%20referents%20regionaux.pdf> [↑](#footnote-ref-29)