Matrice

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

**MODELE DE CHARTE D’IDENTITOVIGILANCE**

# Table des matières

[INFORMATIONS RELATIVES AU DOCUMENT MODELE 3](#_Toc103162635)

[CHARTE D’IDENTITOVIGILANCE 4](#_Toc103162636)

[1. INTRODUCTION 4](#_Toc103162637)

[2. POLITIQUE D’IDENTITOVIGILANCE 4](#_Toc103162638)

[1. Définition et objectifs 4](#_Toc103162639)

[2. Engagement de la structure 5](#_Toc103162640)

[3. Le périmètre d’action de la politique 5](#_Toc103162641)

[3. GOUVERNANCE DE L’IDENTITOVIGILANCE 6](#_Toc103162642)

[1. Le comité de pilotage de l’identitovigilance 6](#_Toc103162643)

[2. Le référent en identitovigilance 7](#_Toc103162644)

[3. Les correspondants en identitovigilance 7](#_Toc103162645)

[4. Les référents logiciels 8](#_Toc103162646)

[4. DEFINITIONS ET TERMINOLOGIE 8](#_Toc103162647)

[1. Identification 8](#_Toc103162648)

[2. Identité et identifiant numériques 9](#_Toc103162649)

[3. Domaine d’identification et de rapprochement 9](#_Toc103162650)

[4. Traits d’identification 9](#_Toc103162651)

[5. Statuts des identités 9](#_Toc103162652)

[6. Doublons, fusions et collisions 10](#_Toc103162653)

[5. LA GESTION DE L’IDENTITE 10](#_Toc103162654)

[1. Le domaine d’identification 10](#_Toc103162655)

[2. Les identifiants utilisés dans l’établissement 10](#_Toc103162656)

[3. Les lieux de création de l’identité 11](#_Toc103162657)

[4. Les traits d’identification 11](#_Toc103162658)

[5. Recherche, création, qualification d’une identité 13](#_Toc103162659)

[6. Le maintien de la qualité du référentiel identité 16](#_Toc103162660)

[7. Droits d’identification 17](#_Toc103162661)

[6. FIABILISATION DE L’IDENTIFICATION SECONDAIRE 19](#_Toc103162662)

[1. La photographie d’identification 19](#_Toc103162663)

[2. Identification de l’usager lors des prestations d’accompagnement et de soins 19](#_Toc103162664)

[3. Identification des documents du dossier de l’usager 20](#_Toc103162665)

[4. Les supports physiques d'identification 20](#_Toc103162666)

[7. LA GESTION DOCUMENTAIRE (GED) 21](#_Toc103162667)

[1. Procédures 21](#_Toc103162668)

[2. Modes opératoires 21](#_Toc103162669)

[3. Enregistrements 22](#_Toc103162670)

[8. PILOTAGE 22](#_Toc103162671)

[1. Indicateurs d’identification primaire 22](#_Toc103162672)

[2. Indicateurs d’identification secondaire 23](#_Toc103162673)

[3. Formation du personnel 23](#_Toc103162674)

[4. Évaluation et amélioration des pratiques professionnelles 23](#_Toc103162675)

[9. LA GESTION DES RISQUES 24](#_Toc103162676)

[1. La gestion des risques a priori 24](#_Toc103162677)

[2. La gestion des risques *a posteriori* 27](#_Toc103162678)

[10. LA FORMATION ET LA SENSIBILISATION DES ACTEURS 27](#_Toc103162679)

[3. Action de sensibilisation et de communication auprès des professionnels 28](#_Toc103162680)

[11. RESPECT DES DROITS DE L’USAGER, INFORMATION SENSIBILISATION 28](#_Toc103162681)

[1. Respect du RGPD 28](#_Toc103162682)

[2. Information et sensibilisation des usagers 29](#_Toc103162683)

[12. ACTUALISATION DE LA CHARTE ET DE LA POLITIQUE D’IDENTITOVIGILANCE 29](#_Toc103162684)

[13. REFERENCES BIBLIOGRAPHIQUES 30](#_Toc103162685)

# INFORMATIONS RELATIVES AU DOCUMENT MODELE

**PREAMBULE**

Une charte est un document officiel destiné à établir des objectifs, des valeurs, des principes ou des règles partagées.

Dans le monde de la santé, elle est utilisée pour définir des engagements pris par les signataires vis-à-vis des usagers (charte des droits et libertés de la personne accueillie…) ou des professionnels (charte pour le signalement des événements indésirables, charte informatique…).

La charte d’identitovigilance est un document qui a pour objet de formaliser la politique de chaque structure en matière d’identification des usagers pris en charge. Elle définit le périmètre et les conditions d’enregistrement, d’utilisation et de sécurisation des données d’identité ainsi que l’information des parties prenantes. Elle fait référence aux documents spécifiques qui développent les aspects techniques et opérationnels : procédures, protocoles, modes opératoires…

Afin d’accompagner les établissements et services médico-sociaux, l’ANAP propose un modèle de document reprenant les éléments à retrouver de manière obligatoire dans la charte locale, selon les dispositions définies dans le Référentiel national d’identitovigilance (RNIV). Ce modèle de charte d’identitovigilance est à adapter par chaque service et établissement médico-social en fonction de ses spécificités organisationnelles et techniques.

**MODE D’EMPLOI DU DOCUMENT**

Les indications en *bleu italique* sont destinées à apporter une aide à la rédaction, ou des conseils à l’établissement ou service. Elles devront être supprimées après que la charte de la structure a été rédigée.

Le *vert italique* indique les espaces où il est attendu le nom de la structure ou des applications utilisées.

Les parties en *rouge italique* indiquent les parties dont le développement est proposé pour personnaliser les éléments spécifiques à la structure.

Il est conseillé aux structures de suivre le plan proposé afin de balayer l’ensemble de la thématique identitovigilance dans la charte.

# CHARTE D’IDENTITOVIGILANCE

## INTRODUCTION

*Objet du chapitre : décrire les objectifs de la charte d’identitovigilance.*

*Exemple de rédaction :*

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 *nom de la structure* 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…

## POLITIQUE D’IDENTITOVIGILANCE

### Définition et objectifs

*Objet du chapitre : définir l’identitovigilance et décrire les objectifs de la structure en termes de bonnes pratiques d’identification des résidents/usagers/personnes accompagnées.*

*Exemple de rédaction :*

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.

### Engagement de la structure

*Objet du chapitre : préciser la politique mise en œuvre dans la structure en matière d’identitovigilance et rappeler son lien avec le Référentiel National d’Identitovigilance*.

*Exemple de rédaction :*

*Nom de la structure* 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).

### Le périmètre d’action de la politique

#### 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 *nom de la structure* :

*Décrire ici les modalités de prises en charge :*

* *accueil de jour ;*
* *accueil temporaire,*
* *accueil ou hébergement permanent…*
* *semi-internat ;*
* *internat …*

#### 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) :

*Citer la liste des catégories professionnelles participant à l’identification de l’usager :*

* *professionnels de santé (médecins, infirmiers, aide-soignant…) ;*
* *professionnels de l’accompagnement (moniteurs d’atelier, moniteurs éducateurs, éducateurs spécialisés…)*
* *secrétaires médicales, administratives et l’accueil ;*
* *brancardiers ou ambulanciers ;*
* *personnels des services informatiques ;*
* *correspondants libéraux associés à la prise en charge ESMS-ville-hôpital…*

#### 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 *nom de la structure*, qu’elles soient ou non alimentées par le référentiel d’identités.

La liste des applications informatiques partageant des données de santé nominatives est tenue à jour sous l’autorité du responsable ou du directeur des systèmes d’information (RSI).

## GOUVERNANCE DE L’IDENTITOVIGILANCE

*Objet du chapitre : préciser la structuration de l’identitovigilance en termes :*

* *de conduite de la politique d’identitovigilance dans la structure ;*
* *de traitement des signalements d’erreurs constatées ;*
* *d’analyse et de correction des anomalies dans la base (doublons, fusions…).*

*Nom de la structure* 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) ;*
* un niveau opérationnel, représenté par le référent en identitovigilance et ses correspondants locaux (mention à supprimer si la structure n’a pas identifié de correspondants locaux) .

Au niveau du groupe *nom de l’OG*, ces instances sont coordonnées au niveau de par un comité de coordination (*nom de l’instance*).

### Le comité de pilotage de l’identitovigilance

*Aide à l’organisation : En fonction de sa taille (structure appartenant à une OG ou non), de son organisation, la structure peut choisir de prendre en compte l’identitovigilance au sein d’un comité existant (comité qualité gestion des risques, comité de direction...) ou de créer un comité spécifique.*

#### Missions

Le comité de pilotage de l’identitovigilance (*COPIL*) est chargé de :

* valider la politique d’Identitovigilance de la structure ;
* arrêter l’organisation à mettre en œuvre (organisation, moyens, missions confiées) ;
* arrêter le plan d’action annuel ou pluriannuel relatif au déploiement des bonnes pratiques d’identification ;
* mettre en place le système permettant le pilotage de la thématique (indicateurs, retours d’information du terrain…) ;
* analyser et résoudre les difficultés signalées ;
* formaliser un bilan annuel de la thématique.

*Préciser si un règlement précisant le fonctionnement du comité a été formalisé.*

*La structure peut faire le choix de décrire ici l'organisation ou de produire un document dédié.*

#### Composition

Le *COPIL* est composé par *(à personnaliser :*

* *le directeur ou son représentant ;*
* *un représentant des professionnels de santé ;*
* *un représentant des professionnels d’accompagnement ;*
* *le responsable de la démarche qualité gestion des risques ;*
* *le référent en identitovigilance ;*
* *le directeur ou le responsable des systèmes d’information (RSI) ou son représentant ;*
* *le délégué à la protection des données (DPD) de la structure ;*
* *le responsable administratif charge des admissions ;*
* *un représentant des structures partenaires (sous-traitants et prestataires), si pertinent ou si possible.*

La composition nominative est actualisée annuellement et disponible dans la gestion documentaire (*nom de la GED si applicable*).

#### Fréquence des réunions

Le *COPIL* est réuni au moins deux fois par an sur convocation du directeur.

### Le référent en identitovigilance

*Objet du chapitre : préciser les missions du référent en identitovigilance de la structure.*

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 privilégié́ 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 *nom de la structure*, 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.

### Les correspondants en identitovigilance

*Objet du chapitre : préciser les missions des professionnels correspondants de l’établissement, structure ou service identifiés dans les services et les structures partenaires (si applicable). Ce chapitre est à supprimer si la structure ne désigne pas de correspondants en identitovigilance.*

*Exemple de rédaction :*

* **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, *le cas échéant*. 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 externes**

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 *(préciser le lieu).*

### Les référents logiciels

*Objet du chapitre : préciser le rôle des référents logiciels.*

*Exemple de rédaction :*

Le système d’information de la structure réunit plusieurs applications informatiques dédiées à des tâches spécifiques d’identification. Pour assurer la cohérence de l’ensemble des logiciels destinés à traiter des informations personnelles d’usagers, chaque application est pilotée par un référent logiciel.

Les différents référents logiciels s’assurent de la qualité des flux de transmission des données d’identification et de leur bonne intégration dans les services clients. Ce contrôle fait intervenir, si besoin, les référents en identitovigilance concernés.

## DEFINITIONS ET TERMINOLOGIE

*Objet du chapitre : préciser les définitions des termes employés dans les documents d’identitovigilance de l’établissement, structure ou service.*

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.

### 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.

### 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.

### 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 ».

### 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.

### 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.

### 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.

## LA GESTION DE L’IDENTITE

*Objet du chapitre : décrire la gestion de l’identité au sein de l’établissement, structure ou service, en termes de traits utilisés, de système d’information, de pratiques.*

*Exemple de rédaction :*

### Le domaine d’identification

*Objet du chapitre : décrire le domaine d’identification.*

*Le fait de disposer d’un référentiel unique identité est une exigence du RNIV. La présence d’un référentiel unique d’identité permet de sécuriser l’utilisation des identités numériques.*

*Si la structure ne dispose pas d’un référentiel unique d’identité, il est nécessaire de décrire ici les outils non alimentés par le référentiel et dans le chapitre gestion des risques, il faudra décrire les process mis en œuvre pour sécuriser l’identification de l’usager.*

*Indiquer ici le nom de votre structure* dispose d’un référentiel unique d’identité pour toutes les applications participant au processus de soins et d’accompagnement. L’ensemble des applications est alimenté en identité par le référentiel unique d’identité *mettre ici le nom du référentiel*. La cartographie applicative du *indiquer ici le nom de votre structure* (*renvoyer à la cartographie applicative par un lien hypertexte par exemple*) décrit les interfaces existantes entre les applicatifs utilisés.

### Les identifiants utilisés dans l’établissement

*Objet du chapitre : décrire les identifiants utilisés dans l’établissement.*

*Point d’attention, le matricule INS pouvant varier dans certains cas, il n’est pas considéré ici comme un identifiant mais comme un trait strict de d’identité.*

Les identifiants numériques utilisés dans l’établissement sont :

* l’identifiant permanent patient (IPP), identifiant unique du dossier de l’usager et associé à son identité ;
* l’identifiant d’épisode patient (IEP) ou numéro de séjour, qui identifie le séjour ou la venue et est relié à l’IPP du dossier.

Un nouvel IEP est créé à chaque venue de l’usager.

### Les lieux de création de l’identité

*Objet du chapitre : décrire les lieux de création de l’identité dans l’établissement. L’établissement supprime les items non pertinents et adapte le tableau en fonction de ses pratiques.*

*Il est rappelé que la création des identités par les soignants ou professionnels éducatifs doit être limitée à des cas très particuliers.*

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Service lieux** | **Période** | **Fonction des personnels** | **Commentaire** |
| Secrétariat d’admission | Heures ouvrables | Secrétaire médico-sociale |  |
| *A compléter* | *A compléter* | *A compléter* |  |

### Les traits d’identification

*Objet du chapitre : préciser les traits d’identification et les règles de saisie de l’identité retenues dans la structure.*

*Indiquer ici le nom de la structure* respecte les exigences du RNIV en matière de traits d’identification. Les traits d’identification utilisés sont les suivants :

#### 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).

#### Traits complémentaires

*La structure adaptera les traits complémentaires proposés en fonction de ses pratiques.*

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) ;
* Code postal de la commune de naissance (pour les usagers nés en France exclusivement) ;
* 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).

#### Politique de la structure concernant la saisie des noms et prénoms utilisés

*Objet du chapitre : ce chapitre vise à décrire la politique adoptée par l’établissement.*

*Pour mémoire : le RNIV rend possible la saisie dans les champs nom et prénom utilisés d’éléments ne figurant pas sur la pièce d’identité présentée par l’usager. La structure doit choisir :*

* *soit de recopier à l’identique une pièce d’identité ;*
* *soit de permettre la saisie d’un nom ou d’un prénom non présent sur une pièce d’identité ;*
* *soit de permettre de ne pas saisir un nom ou un prénom présent sur une pièce d’identité.*

*Trois rédactions sont proposées selon les choix qui peuvent être faits par l’établissement, la structure ou le service. L’établissement supprime les éléments proposés non pertinents.*

*Mettre ici le nom de la structure* : a fait le choix de :

*Choix 1 possible : 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),
* ce prénom, bien qu’il ne fasse pas partie des prénoms de naissance est explicitement mentionné sur la pièce d’identité (prénom usuel : XXX).

*Choix 2 possible : ne pas saisir un nom utilisé y compris s’il est présent sur une pièce d’identité si l’usager ne le souhaite pas.*

L’établissement a mis en place une organisation permettant lors des éventuels contrôles à distance de l’identité de s’assurer qu’il ne s’agit pas d’une erreur du professionnel de l’accueil. (*L’établissement décrit ici l’organisation adoptée : document rempli par l’usager et scanné dans le dossier par exemple*).

*Choix 3 possible : saisir un nom utilisé ou un prénom utilisé non présents sur la pièce d’identité, à la demande de l’usager.*

L’établissement a mis en place une organisation permettant lors des éventuels contrôles à distance de l’identité de s’assurer qu’il ne s’agit pas d’une erreur du professionnel de l’accueil. (*L’établissement décrit ici l’organisation adoptée : document rempli par l’usager et scanné dans le dossier par exemple*).

*Si la structure pratique le double nommage, (saisie systématique d’un nom utilisé y compris s’il est identique au nom de naissance et/ou saisie systématique d’un prénom utilisé y compris s’il est identique au premier prénom de naissance) il est nécessaire de l’indiquer ici.* *La pratique du double nommage n’est pas conseillée, cependant les structures peuvent être contraintes par les fonctionnalités de leur système d’information et en particulier de leurs outils métier.*

*Choix 1 possible : La structure a fait le choix de pratiquer le double nommage en ce qui concerne les champs (la structure adapte la proposition et supprime par exemple le double nommage pour le champ prénom utilisé, si elle ne le pratique pas) :*

* nom utilisé : ce champ sera systématiquement rempli y compris si l’usager utilise uniquement son nom de naissance dans la vie courante (recopie du nom de naissance dans le champ nom utilisé) ;
* prénom utilisé : ce champ sera systématiquement rempli y compris si l’usager utilise uniquement son premier prénom de naissance dans la vie courante (recopie du premier prénom de naissance dans le champ prénom utilisé).

*Choix 2 possible : la structure ne pratique pas le double nommage :*

* 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*.*

### Recherche, création, qualification d’une identité

#### 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).

#### Recherche d’une identité

*Objet du chapitre : Décrire les principes de recherche d’une identité dans l’établissement.*

*L’établissement adapte la rédaction proposée en fonction de ses pratiques. La recherche par date de naissance est recommandée par le RNIV.*

Conformément au RNIV, la recherche d’une identité est réalisée par la saisie de la date de naissance.

Compte tenu de la taille du référentiel identité et afin de diminuer les temps de recherche, l’établissement a fait le choix de compléter la date de naissance par les x premiers caractères du nom et/ou par les y premiers caractères du prénom.

*La structure adapte le paragraphe ci-dessous selon les fonctionnalités proposées par le logiciel*.

Le système d’information permet la recherche d’une chaine de caractères à la fois dans les champs nom de naissance et 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.

*Il est possible de rajouter la phrase suivante si historiquement la structure a enregistré des identités par lecture de la carte vitale par exemple*. Compte tenu des particularités du référentiel identité et de l’historique de la gestion des identités dans la structure, si l’usager n’est pas retrouvé en utilisant la recherche par date de naissance, une seconde recherche sera réalisée sans utiliser le critère date de naissance.

#### Création d’une identité

*Objet du chapitre : décrire les principes 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 obligatoirement complétés par :

* la liste des prénoms de naissance ;
* le matricule INS et son OID ;

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

Et par les traits complémentaires suivants (*l’établissement liste ici les traits complémentaires qui doivent être obligatoirement saisis : par exemple*) :

* ville et code postal de naissance
* 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*

*Objet du chapitre : décrire les règles de saisie d’une identité.*

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*

*Objet du chapitre : décrire la politique de la structure concernant l’appel au téléservice et décrire les modalités utilisées pour l’appel.*

*Choix concernant le statut des identités :*

* Choix 1 possible : l’établissement a fait le choix de n’appeler le téléservice que si l’identité de l’usager est au statut identité validée.
* Choix 2 possible : l’établissement a fait le choix d’appeler le téléservice pour les identités au statut identité provisoire. L’établissement a mis en place une organisation de validation des identités en back office (cf. infra).

*Choix concernant les modalités d’appel :*

* Choix 1 possible : la structure privilégie l’appel au téléservice par lecture de la carte vitale.
* Choix 2 possible : la structure privilégie l’appel au téléservice par saisie des traits.

*Création des identités en heures ouvrables par les professionnels de l’accueil*

*Plusieurs processus de création d’identité sont proposés. L’établissement ne conserve que les éléments adaptés à ses pratiques.*

* Choix 1 possible : Si l’usager est éligible à l’INS, l’établissement a fait le choix de créer une identité à partir des traits récupérés lors de l’appel à l’opération de récupération du téléservice INSi. Cette identité est ensuite complétée par les traits cités infra.
* Choix 2 possible : L’établissement fait le choix de créer systématiquement une identité locale avant de réaliser l’appel au téléservice INSi pour les usagers éligibles.

*Création des identités en heures de permanence des soins par les professionnels présents*

*Proposition d’organisation :*

Les professionnels présents créent une identité locale. La récupération de l’INS est réalisée par la personne en charge des admissions en backoffice 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. Si cette situation est récurrente, un temps de formation pour ces professionnels est à prévoir.

#### Les attributs d’identité

*Objet du chapitre : décrire l’utilisation des attributs de l’identité dans l’établissement. L’établissement modifie la rédaction proposée selon ses pratiques.*

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.

#### Le processus de validation des identités et de qualification de l’INS

*Objet du chapitre : décrire l’organisation de l’établissement pour la validation des identités et la qualification des INS. Il est fortement recommandé qu’un process de validation en FrontOffice s’accompagne d’une demande de vérification des traits saisis par l’usager (sur une planche d’étiquette, sur un document de circulation, une fiche administrative…).*

Choix 1 possible : 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 sur un support (préciser ici le support utilisé).

Choix 2 possible : La validation des identités est réalisée en back office par le COPIL[[1]](#footnote-2) après réalisation d’un contrôle de cohérence entre l’identité numérique et l’identité présente sur la pièce d’identité. La pièce d’identité numérisée est disponible dans le référentiel identité.

#### Les dispositifs d’identification à haut niveau de confiance

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, 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.

L’établissement dispose d’un outil de numérisation des pièces d’identité. Ces pièces sont conservées dans les conditions précisées dans la *FIP06 Gestion des copies de pièces d’identité dans le système d’information proposée par le réseau 3RIV* (*Cette mention est à supprimer si la structure ne dispose pas d’outil de numérisation*).

#### Les identités particulières

*Objet du chapitre : décrire de façon macroscopique les identités particulières pouvant être utilisées par l’établissement. Le cas échéant, supprimer les paragraphes non applicables.*

L’établissement peut utiliser des identités fictives à la demande d’un usager qui souhaite être pris en charge sans divulgation de son identité.

La création de ces identités fictives fait l’objet d’une procédure, d’une formation particulière des personnels.

*La structure peut donner ici les grands principes de création des identités fictives ou renvoyer à la procédure ad hoc. Le fait de donner les grands principes dans la charte, ne dispense pas de disposer d’une procédure spécifique.*

*La procédure identité fictive doit prévoir en particulier :*

* Les règles de nommage : il est recommandé d’utiliser une date de naissance cohérente avec l’âge apparent de l’usager, de compléter la chaine de caractère choisie pour le nom par un numéro incrémental (date du jour par exemple). Le réseau 3RIV propose plusieurs fiches pratiques et un memento sur lesquels l’établissement peut s’appuyer pour définir les règles de nommage.
* La procédure de rectification de ces identités (hors cas légaux d’anonymat) et d’information des partenaires.

#### Identification primaire sans présence physique de l’usager

Identités transmises à un sous-traitant, télé-expertise…

Conformément au RNIV, l’établissement a inclus une clause de confiance dans les contrats qui le lient à ses sous-traitants ou partenaires (pharmacie, laboratoire, …).

### Le maintien de la qualité du référentiel identité

Objet du chapitre : décrire l’organisation du signalement des anomalies et de leur traitement.

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.

*Il est conseillé de disposer de deux procédures, une de signalement à destination des personnels de l’établissement, l’autre de traitement à destination des personnels de la COMIV.*

*La procédure de signalement doit comporter :*

* 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…)

*L’établissement peut décrire ici brièvement le circuit par exemple :*

L’établissement dispose d’un outil informatisé de signalement des anomalies. Les professionnels utilisent un formulaire dédié. Les anomalies traitées alimentent le tableau de bord de pilotage….

### Droits d’identification

*Objet du chapitre : décrire les droits liés à l’utilisation des identités dans l’établissement.*

*Un exemple de présentation sous forme de tableau vous est proposé ci-dessous, renseigné avec les organisations les plus courantes. L’établissement doit modifier le tableau proposé en fonction de son organisation.*

*Pour mémoire, il est fortement conseillé de limiter les droits de modifications d’identité (bureau des entrées et COMIV). Il est préconisé de ne pas donner les droits d’appel au téléservice INSi aux soignants et professionnels d’accompagnement (qui ne sont pas des professionnels de l’accueil).*

Les droits d’identification des personnels sont décrits dans le tableau ci-dessous.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Service lieux** | **Application utilisée** | **Recherche et consultation d’identité** | **Création identité locale** | **Appel au téléservice INSi** | **Modification d’identité** | **Validation d’identité** | **Fusion et défusion de collision** | **Déqualification suppression d’une INS** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

## FIABILISATION DE L’IDENTIFICATION SECONDAIRE

*Objet du chapitre : décrire les moyens mis en œuvre par la structure pour fiabiliser l’identification secondaire.*

### La photographie d’identification

*Si la structure n’utilise pas de photographie de l’usager présente dans le dossier pour l’identifier, ce chapitre est à supprimer.*

*Indiquer ici le nom de la structure* utilise comme dispositif d’identification de l’usager une photographie présente dans son dossier. L’information de l’usager, la prise de la photographie, l’intégration dans le dossier patient et les éléments de contrôle sont formalisés au sein d’une procédure.

Les documents qualité nécessaires doivent être rédigés et comprendre :

* la fiche d'information de l’usager ou de sa famille ou livret d’accueil ;
* les éléments de traçabilité de la décision de l’usager et le support d'enregistrement (dossier papier, dossier de soin informatisé).

Dans chaque structure de santé, le comité d'éthique et/ou la CDU doivent être consultés concernant l'utilisation d'une photographie. Eléments à préciser dans la procédure « dispositif d’identification » de la structure :

* usagers ou services concernés;
* service en charge de la photographie ; insertion de la photographie dans le dossier ;
* modalités d’information de l’usager et du recueil du consentement (droit à l’image) ;
* traçabilité dans le dossier de la décision de l’usager et du consentement ;
* périodicité de renouvellement de la photographie ;
* conduite à tenir en cas de refus de l’usager de prise de photographie.

L’utilisation d’une photographie d’identification nécessite l’information de l’usager et l’obtention d’un accord écrit de sa part, mentionnant les éléments de droits à l’image. Cet accord est conservé dans le système d’information. L’accord de l’usager doit être renouvelé à chaque épisode d’hospitalisation ou selon une périodicité à déterminer par l’établissement. La photographie doit être considérée comme une donnée à caractère personnel (article 4 RGPD) et la finalité doit être précisée. La conservation d’une photographie doit être mentionnée dans le registre de traitement de l’établissement.

### Identification de l’usager lors des prestations d’accompagnement et de soins

*On entend par prestations d’accompagnement et de soins toutes les prestations réalisées auprès de l’usager : éducatif, médical, paramédical, psychologique, social, transport.*

Chaque soignant, chaque professionnel, 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.

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.

Une procédure est disponible dans la gestion documentaire.

### Identification des documents du dossier de l’usager

*Indiquer ici le nom de la structure* 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.

Décrire ici les moyens mis en œuvre par exemple :

* tous les documents paramétrés dans le DUI et destinés à être imprimés sont identifiés sur toutes les pages par le nom de naissance, le nom utilisé s’il est différent du nom de naissance, le (s) prénom(s) de naissance, la date de naissance le sexe et l'IPP en-tête ou en en pied de page. Si l’usager dispose d’une INS, l’identité comprend également le code du lieu de naissance ainsi que le matricule INS suivi de sa nature (NIR ou NIA).
* la procédure de numérisation des documents dans le DUI est formalisée et limite le risque d’erreur (double contrôle) ;
* les personnels en charge du rangement des documents.

### Les supports physiques d'identification

*Si l’utilisation de supports physiques d’identification n’est pas une pratique actuelle de votre structure, il convient néanmoins d’interroger les situations à risque dans lesquelles un tel dispositif pourrait s’avérer pertinent (exemple : transfert vers un autre établissement).*

*Indiquer ici le nom de la structure* propose aux usagers de porter des bracelets/badges d’identification. Le port du bracelet est obligatoire pour les usagers non communicants (non francophone, confus, inconscient, dément…). L’information de l’usager, la pose du bracelet/badge et les éléments de contrôle sont formalisés au sein d’une procédure.

Si tous les services de la structure ne sont pas concernés par la pose d’un bracelet, lister les services concernés.

Dans la mesure du possible, il ne doit pas y avoir transcription manuelle de l'identité de l’usager sur le bracelet (source d'erreur).

Il faudra privilégier les bracelets imprimés sur une imprimante dédiée à partir des données du SIH ou les étiquettes imprimées à partir du SIH et collées sur le bracelet.

Les documents qualité nécessaires doivent être rédigés et comprendre :

* la fiche d'information de l’usager ou de sa famille ou livret d’accueil ;
* les éléments de traçabilité de la décision de l’usager et le support d'enregistrement (dossier papier, dossier de soin informatisé).

Dans chaque structure de santé, le comité d'éthique et/ou la CDU doivent être consultés concernant l'utilisation d'un bracelet d'identification.

Éléments à préciser dans la procédure « dispositif d’identification » de la structure :

* usagers ou services concernés par la pose du bracelet ;
* service créateur du bracelet ;
* informations contenues dans le bracelet ;
* positionnement du bracelet : sur quel membre le positionner, qui le positionne, à quel moment ;
* modalités d’information de l’usager sur la pose et l’utilisation du bracelet d’identification ; traçabilité dans le dossier de la décision de l’usager ;
* vérification des informations portées sur le bracelet (par qui, quand, comment) ;
* conduite à tenir en cas de refus de l’usager de pose de bracelet (les mesures barrières qui peuvent être mises en place pour sécuriser l’identification en l’absence de bracelet).

## LA GESTION DOCUMENTAIRE (GED)

*Objet du chapitre : rappeler les modalités de gestion de l’ensemble de la documentation en lien avec l’identitovigilance. Il est proposé ici de lister l’ensemble des types de documents utilisés en identitovigilance.*

L’ensemble de la documentation, procédures, modes opératoires, enregistrements, relative à l’identitovigilance sont disponibles dans l’outil de gestion documentaire *mettre ici le nom* de l’outil.

L’alimentation de la GED est sous la responsabilité du service qualité gestion des risques *(préciser la dénomination locale de la fonction)*.

### Procédures

*Objet du chapitre : lister exhaustivement les procédures d’identitovigilance en vigueur dans la structure.*

*Une procédure est un document qualité reprenant les principes des actions et les grandes étapes. A ne pas confondre avec un mode opératoire, document plus court, pouvant comporter des copies d’écran qui guide de façon détaillée l’utilisateur dans la réalisation d’une action.*

*L’établissement supprimera de la liste les procédures non pertinentes au regard de son activité et rajoutera les procédures supplémentaires qu’il jugerait utile.*

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 points d’accueil ;
* Admission d’un usager souhaitant garder l'anonymat ;
* Utilisation d’un dispositif physique d’identification (bracelet d’identification, photographie) ;
* Identification secondaire d’un usager avant tout accompagnement ou soin ;
* Gestion des transferts entre établissements et au sein de l’établissement ;
* 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) ;
* Gestion d’une suspicion de substitution frauduleuse d’identité ;
* Information des partenaires après détection d’une erreur d’identification d’un usager ;
* Gestion des identités dans les logiciels non ou incomplètement interfacés, appartenant à des domaines d’identification différents ou non (obligatoire pour les structures si certains des logiciels participant à la prise en charge de l’usager sont incomplètement interfacés ou ne sont pas interfacés) ;
* 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 ;
* Tests des interfaces d’identités ;
* Procédure de gestion et de contrôle qualité des bases d'identités des professionnels de santé comprenant la procédure de déclaration d’un nouvel agent au sein du SI et la définition des droits d’accès (cette procédure intégrera la gestion des clôtures de compte).

### Modes opératoires

*Objet du chapitre : l’établissement peut détailler ici les modes opératoires disponibles.*

*Les modes opératoires sont des documents opérationnels permettant de préciser la façon de réaliser des actions. Le mode opératoire comporte en général des copies d’écran.*

### Enregistrements

*Objet du chapitre : préciser les enregistrements importants que l’on peut retrouver dans la gestion documentaire. Un enregistrement est un document faisant état de résultats obtenus ou apportant la preuve de la réalisation d’une activité. Les enregistrements doivent être maitrisés (ISO 9001).*

L’établissement liste ici la liste des enregistrements.

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

* documents réglementaires et techniques (fiches du réseau 3RIV, fiches GRIVES…) ;
* comptes rendus de réunion du COPIL ;
* cartographie applicative et schéma des flux ;
* supports de formations ;
* Support de communication et de sensibilisation (affiches, flyers…) ;
* cartes d’identité des indicateurs ;
* 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, …).

## PILOTAGE

*Objet du chapitre : décrire les outils de pilotage de la thématique, indicateurs suivis dans la structure et le mode de suivi, évaluations réalisées plan d’évaluation….*

*Indiquer ici le nom de la structure* suit des indicateurs relatifs à l’identification primaire et à l’identification secondaire.

Chaque indicateur dispose d’une carte d’identité disponible dans la GED.

Les indicateurs sont rassemblés dans un tableau de bord et sont suivis trimestriellement à l’exception du taux de formation du personnel qui est suivi annuellement. Le tableau de bord des indicateurs tenu à jour par la COMIV et présenté à chaque réunion.

### Indicateurs d’identification primaire

Les indicateurs listés dans ce chapitre sont les indicateurs proposés.

Les indicateurs suivis dans la structure sont les suivants (*supprimer de la liste les indicateurs non suivis, rajouter éventuellement des indicateurs suivis qui ne seraient pas listés*) :

* 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 de doublon de flux d’INS ;
* part des doublons d’INS dans les doublons ;
* taux de doublon de flux ;
* taux de doublons traités moins de 72 heures après avoir été dépistés : taux de fusion précoce ;
* nombre et/ou taux de collision ;
* nombre et/ou taux d’usurpation d’identité ;
* rapport fusion sur doublon ;
* taux d’évènements indésirables ayant pour origine une erreur d’identification primaire des usagers ;
* taux d’évènements porteurs de risques ayant pour origine une erreur d’identification primaire des usagers.

### Indicateurs d’identification secondaire

Les indicateurs suivis dans la structure sont les suivants (*supprimer de la liste les indicateurs non suivis, rajouter éventuellement des indicateurs suivis qui ne seraient pas listés*) :

* 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 ;
* suivi des non conformités de biologie médicale ;
* taux de conformité de l’identification des documents du dossier patient ;
* taux de documents référencés avec l’INS.

### Formation du personnel

Les indicateurs listés dans ce chapitre sont les indicateurs proposés. Il est fortement recommandé de suivre l’un ou l’autre des indicateurs proposés.

Les indicateurs suivis dans la structure sont les suivants (*supprimer de la liste les indicateurs non suivis, rajouter éventuellement des indicateurs suivis qui ne seraient pas listés*) :

* taux de formation du personnel par grandes catégories professionnelles ;
* taux de formation du personnel par catégorie spécifique de personnels.

### Évaluation et amélioration des pratiques professionnelles

*Les évaluations listées dans ce chapitre sont des évaluations proposées. Il est fortement recommandé de réaliser annuellement au moins une évaluation relative à l’identification primaire et une évaluation relative à l’identification secondaire.*

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 (*l’établissement modifie le nombre d’évaluations en fonction de ses pratiques*).

Les évaluations / audits pouvant être réalisés sont les suivants :



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.

## LA GESTION DES RISQUES

*Objet du chapitre : ce chapitre vise à décrire les mesures mises en œuvre par l’établissement afin de gérer les risques à priori et a posteriori.*

### La gestion des risques a priori

#### La veille réglementaire et technique

*Objectif du chapitre : décrire les actions de veille réalisées par le référent en identitovigilance.*

*L’établissement adapte la rédaction proposée à ses pratiques.*

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

* journal officiel et bulletins officiels, lettre de l’APM, Hospimedia, … ;
* utilisation des espaces collaboratifs régionaux en identitovigilance
* consultation du site de l’Agence du Numérique en Santé ;
* communication des éditeurs ;
* participation des sessions de formations et d’information ;

#### Modalités d’attribution et de gestion des droits d’accès informatiques

*Objet du chapitre : préciser les principes retenus par la structure pour sécuriser les opérations de création, recherche, modification d’identités (qui détermine les droits ; comment sont formés et gérés les nouveaux arrivants, les intérimaires, les personnels qui quittent définitivement la structure…).*

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. Une attention particulière a été portée à la gestion des copies de pièces d’identité disponibles dans la GED. Seuls les personnels en charge de la création et de la fiabilisation des identités peuvent accéder à ces documents.

Les profils d’accès sont révisés annuellement par *mettre ici l’instance en charge de la révision des profils d’accès*.

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.

Si l’établissement dispose d’un annuaire de gestion des droits d’accès (type annuaire d’entreprise ou IAM), il peut être utile de le préciser ici.

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.

*Décrire ici l’organisation mise en œuvre pour gérer les droits d’accès et les habilitations ou renvoyer à la charte informatique ou à la procédure de sécurité informatique.*

*Par exemple :*

Tout départ de personnel est signalé au service *mettre ici le nom du service* *compétent* 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.

#### Traçabilité des actions

*Objet du chapitre : préciser les modalités d’analyse de l’historique des actions relatives aux données d’identité.*

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 (*à préciser si des accès sont donnés à des fonctions qui peuvent paraître inhabituelles*).

*Préciser ici les fonctions des personnels autorisés par exemple :*

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

*Préciser ici les modalités de contrôle des accès par exemple :*

Des contrôles d’accès aux dossiers sont réalisés :

* aléatoirement de façon semestrielle ;
* 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.

#### Fiabilisation des interfaces d’identités

L’établissement met en œuvre une procédure de test des interfaces d’identités. Ces tests sont conduits par le COPIL, le service informatique et les référents logiciels métiers en relation avec le ou les éditeurs avant la mise en production de la version.

Les tests sont mis en œuvre à chaque changement de version majeure d’un outil ou de l’EAI.

*(si l’établissement ne dispose pas de base de tests, les tests doivent être conduits avant la remise à disposition des applicatifs pour les utilisateurs, l’établissement précise ici son organisation).*

*La procédure doit décrire qui est en charge de la réalisation des tests, à quelles occasion les tests sont réalisés, quels sont les tests réalisés, quelle est la traçabilité.*

#### Sécurisation de l’identité dans les logiciels non ou incomplètement interfacés

*(Ce chapitre doit être présent si les structures ne disposent pas d’un référentiel unique d’identité pour toutes les applications participant au processus de soin et d’accompagnement.)*

*Objet du chapitre : décrire les mesures organisationnelles et techniques mises en place pour s’assurer que malgré l’absence d’interface ou la présence d’interfaces incomplètes, la même identité est utilisée pour le même usager dans tous les applicatifs*

*Exemple de mesure pouvant être mise en place :*

* réalisation d’un contrôle périodique de la cohérence des bases identités (logiciel d’identitovigilance permettant la comparaison des bases ;
* circuit de transmission de l’information éprouvé pour répercuter les fusions, les décollisions, les modifications de l’identité…

#### Détection des utilisations frauduleuses d’identités

*Objet du chapitre : faire un focus sur le risque d’utilisation frauduleuse d’identité. Ce chapitre est intéressant pour les établissements à risque (par exemple : usagers en situation de précarité sociale).*

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.

*Pour mémoire (extrait du RNIV 2) : La conduite à tenir lors d’une suspicion de fraude comprend des mesures de sécurisation telles que :*

* 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…).

*Bien que ce chapitre ne concerne pas le secteur médico-social, il peut néanmoins être un appui aux professionnels pour mettre en place les conduites à tenir en cas de besoin.*

### La gestion des risques *a posteriori*

*Objet du chapitre : préciser le dispositif mis en œuvre pour gérer les signalements des événements indésirables en relation avec l’identitovigilance. L’établissement adapte la rédaction proposée en fonction de son organisation et de ses pratiques.*

*Il est obligatoire de conduire une analyse des EIG.*

L’établissement met en œuvre un système de signalement des événements indésirables, piloté par le responsable du service qualité et gestion des risques. 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 (*préciser ici les principaux partenaires de l’établissement sous-traitants, 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 (préciser ici la méthode mise en œuvre, ALARM…). Les évènements porteurs de risques récurrents sont également analysés en comité de retour d’expérience.

Le référent en identitovigilance et le COPI ont 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 (*mettre ici la périodicité de réactualisation*) la politique d’identitovigilance de l’établissement.

## LA FORMATION ET LA SENSIBILISATION DES ACTEURS

*Objet du chapitre : décrire les modalités de formation et de sensibilisation des professionnels.*

*Le texte proposé est une base indispensable à compléter par l’’établissement.*

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

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 des étudiants (*lister ici les catégories d’étudiants formés en ayant à l’esprit que la formation des internes est indispensable*) est organisée par la COMIV en collaboration avec le comité pédagogique.

La formation est tracée : *préciser ici les modalités de traçabilité de la formation*, idéalement émargement, tenue d’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.

*L’établissement décrit ici les modalités d’organisation des sessions de formation par exemple :*

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.

### Action de sensibilisation et de communication auprès des professionnels

*Ce chapitre vise à présenter les actions de communication et de sensibilisation menées*

*Des actions de sensibilisation sont menées dans l’établissement : lister ici les actions menées :*

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

## RESPECT DES DROITS DE L’USAGER, INFORMATION SENSIBILISATION

### Respect du RGPD

*Objet du chapitre : préciser les modalités mises en œuvre par la structure pour la mise en conformité du traitement des données personnelles informatisées avec le règlement général de protection des données.*

*Exemple de rédaction :*

*Mettre ici le nom de l’établissement, structure ou service* 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), y compris pour l’utilisation de ces données dans le cadre de l’utilisation des services régionaux (à conserver si l’établissement utilise ou alimente des services régionaux, via trajectoire, e parcours ou télémédecine, dossier communicant de cancérologie, ...).

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…

*Une fiche pratique proposée par le 3RIV est disponible pour vous aider à rédiger les documents d’information de l’usager.*

### Information et sensibilisation des usagers

*Objet du chapitre : préciser les modalités d’information des usagers sur l’identitovigilance primaire et secondaire et en particulier sur la gestion de leurs données d’identité. L’établissement modifie/complète ce chapitre selon les moyens de communication disponibles dans la structure.*

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 ;
* ils sont envoyés dans les mails de confirmation de prise de rendez-vous en ligne…

## ACTUALISATION DE LA CHARTE ET DE LA POLITIQUE D’IDENTITOVIGILANCE

*Objet du chapitre : préciser les modalités de réactualisation de la charte et de la politique.*

La politique et la charte sont actualisées périodiquement (mettre ici la périodicité de révision) 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.

## REFERENCES BIBLIOGRAPHIQUES

*Seules sont reprises ici les références bibliographiques majeures.*

*L’ensemble des références présentes dans le volet 1 du RNIV doivent être consultées et à disposition de la structure.*

Charte d’identitovigilance du GRIVES PACA [Accueil - GRIVES (sante-paca.fr)](https://grives.sante-paca.fr/)

Charte d’identitovigilance du Comité technique régional d’identitovigilance de Nouvelle-Aquitaine [Charte d'identitovigilance | identitovigilance (identito-na.fr)](https://www.identito-na.fr/charte-identitovigilance)

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.

1. Le terme COPIL peut être remplacé par Référent en identitovigilance ou correspondant en identitovigilance en fonction de l’organisation mise en place [↑](#footnote-ref-2)