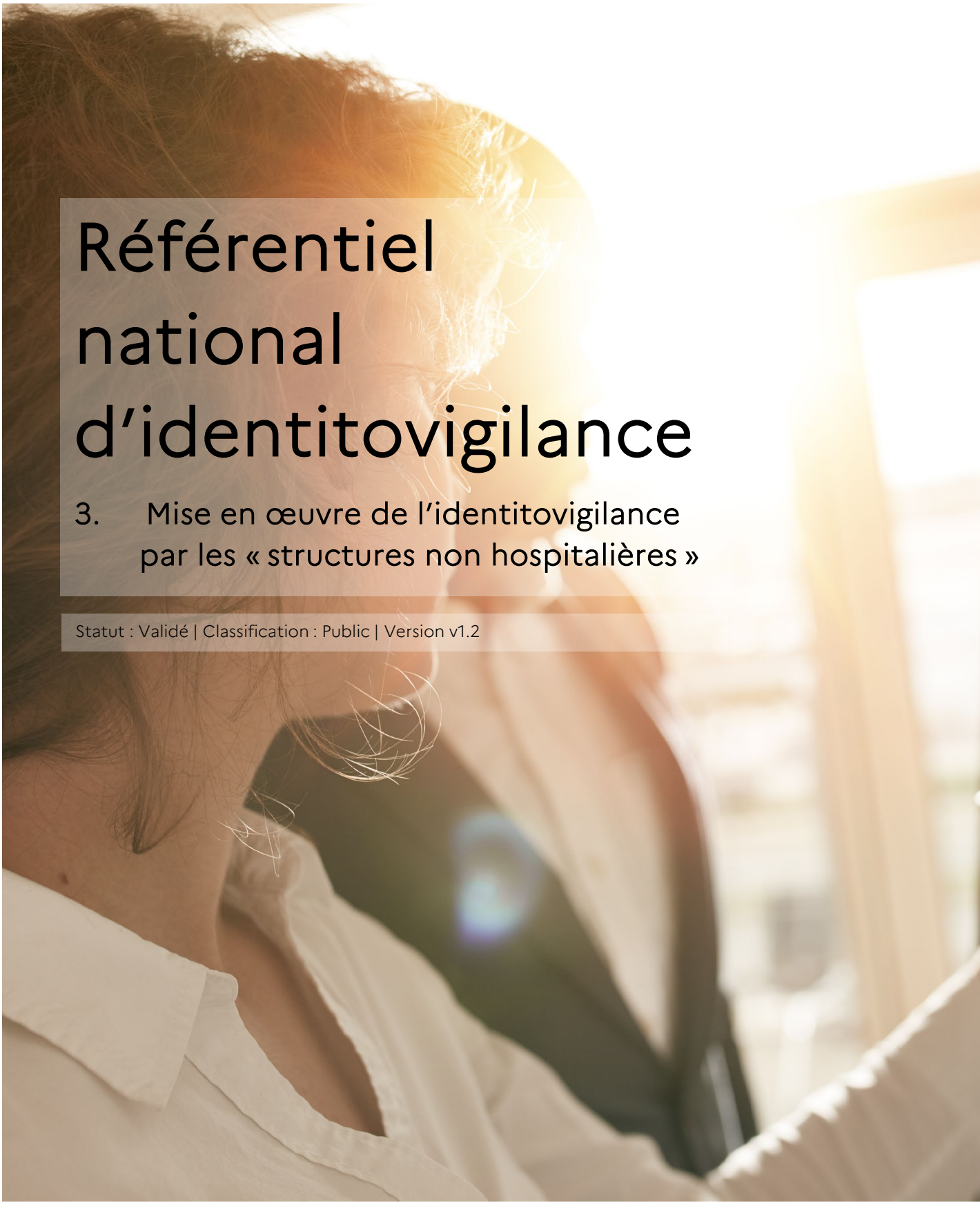
MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

AGENCE
DU NUMÉRIQUE
EN SANTÉ



Référentiel national d'identitovigilance

3. Mise en œuvre de l'identitovigilance par les « structures non hospitalières »

Statut : Validé | Classification : Public | Version v1.2

SOMMAIRE

Contributeurs

Dr Soraya AÏOUAZ, ARS ARA

M. Raphaël BEAUFFRET, DNS

Mme Elsa CREACH, ANS

Mme Céline DESCAMPS, CRIV NA

M. Thierry DUBREU, GRADeS IDF (SESAN)

Dr Gilles HEBBRECHT, DGOS

Dr Christine LECLERCQ, GRADeS Occitanie (e-santé Occitanie)

Mme Bérénice LE COUSTUMER, DGOS

M. Mikaël LE MOAL, DGOS

Dr Isabelle MARECHAL, CHU Rouen

Mme Christelle NOZIERE, CRIV NA

Dr Manuela OLIVER, GRADeS PACA (ieSS)

M. Loïc PANISSE, GRADeS Occitanie (e-santé Occitanie)

M. Bertrand PINEAU, GRADeS IDF (SESAN)

Mme Isabelle STACH, GRADeS Occitanie (e-santé Occitanie)

Dr Sylvie RENARD-DUBOIS, DGOS

M. Michel RAUX, DGOS

Dr Bernard TABUTEAU, CRIV NA

Mme Charlotte VOEGTLIN, GCS Tesis, La Réunion

L'équipe remercie les différents professionnels qui ont contribué à améliorer ce document lors de la phase de concertation.

Historique des versions

Version	Date	Contexte
1.0	18/12/2020	1ère mise en ligne du document
1.2	20/05/2021	Mise à jour, notamment suite avis CNIL

1 Introduction

1.1 Objet du document

Le présent document a pour objet de donner des pistes d'organisation de la gestion des risques relatifs à l'identification des usagers dans les *structures non hospitalières* (SNH), terme proposé pour regrouper l'ensemble des structures d'exercice collectif dans les domaines sanitaire et médico-social. Il est rédigé en complément des règles et recommandations relatives à l'identitovigilance éditées dans le document socle du RNIV (RNIV 1) et n'a pas vocation à se substituer aux recommandations de bonne pratique et règlements spécifiques applicables à certaines activités (exemple : laboratoires de biologie médicale, télémédecine, etc.).

Il constitue une adaptation des préconisations faites dans le 2e volet du référentiel national d'identitovigilance (RNIV 2), consacré aux établissements de santé, dont il partage le plan général de présentation. Il est annexé au référentiel « Identifiant national de santé », qu'il vient compléter.

Des informations et fiches pratiques complémentaires pourront être proposées au niveau régional et/ou national, pour préciser certaines notions qu'il n'est pas possible de développer dans ce document.

1.2 Structures concernées

Les structures concernées par les préconisations du présent document sont :
- les établissements et services médico-sociaux (ESMS) ;
- les structures de santé d'exercice coordonné (ESP, MSP, CDS, CPTS, SCM…) de plus de 10 équivalents temps plein (ETP) ;
- les dispositifs de coordination des parcours de santé (DAC…) ;
- toutes structures réalisant des actes ou soins et employant plus de 10 professionnels ;
- les prestataires qui réalisent des actes sans contact direct avec les usagers…

Les agences régionales de santé (ARS), sur avis éventuel de l'instance stratégique régionale d'identitovigilance, peuvent toutefois décider :
- de rendre ce 3e volet du RNIV applicable à certains établissements de santé qui, du fait de leur taille réduite ou du faible turnover de leurs patients (exemples : USLD, certaines unités de psychiatrie, unités de dialyse) relèvent plutôt des mesures simplifiées développées dans le présent document ;
- de demander au contraire à certaines SNH, du fait d'un risque élevé d'erreurs en termes de fréquence ou de gravité potentielle (exemple : groupe de radiologie effectuant des actes de radiothérapie), de mettre en œuvre l'ensemble des préconisations faites aux établissements de santé dans le 2e volet du RNIV.

Remarque : les cabinets libéraux d'exercice individuel ne sont pas concernés par ce document mais par un volet spécifique du RNIV, à paraitre. C'est également le cas pour les acteurs libéraux exerçant en société d'effectif limité (10 équivalents temps plein ou moins), sauf s'ils choisissent volontairement de conduire une politique qualité plus exigeante.

1.3 Rappel des enjeux

La bonne identification d'un usager est un facteur clé de la sécurité de son parcours de santé. Elle doit être le premier acte d'un processus qui se prolonge tout au long de sa prise en charge par les différents professionnels impliqués, quelle que soit leur spécialité (intervenants administratifs, médicaux, paramédicaux, assistants médico-administratifs, médico-techniques, médico-sociaux ou sociaux), le type de prise en charge (hospitalier, médecine de proximité, médico-social, social) et les modalités d'exercice (structure privée ou publique).

La responsabilité des acteurs de santé et des dirigeants de structures pourrait être mise en cause s'il s'avérait que le défaut de mise en œuvre des bonnes pratiques d'identification était à l'origine d'un dommage ou de la mise en danger d'un usager.

1.4 Périmètre de l'identitovigilance

L'identitovigilance est définie comme l'organisation et les moyens mis en œuvre pour fiabiliser 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 de la structure afin que les données de santé enregistrées soient accessibles chaque fois que nécessaire ;
- d'*identification secondaire* qui permet de garantir que le bon soin est administré au bon patient/résident.

2 Politique et gouvernance

Ce chapitre est en lien avec l'organisation de l'identitovigilance à l'échelon « local » (site géographique) ou « territorial » (établissement ou service réparti sur plusieurs sites géographiques, groupe d'établissements partageant la même politique d'identitovigilance, département). Le terme « structure » s'applique indifféremment à ces différents niveaux d'organisation.

2.1 Politique d'identitovigilance

2.1.1 Comment formaliser la politique d'identitovigilance ?

La politique d'identitovigilance doit être intégrée à la politique qualité et sécurité conduite par la structure ou par le groupe auquel elle appartient. [Reco SNH 01]

Elle est décrite dans le projet d'établissement ou dans le *projet de santé*.

Elle a pour objet de favoriser le déploiement de la culture de sécurité auprès de tous les acteurs concernés, qu'ils soient internes à la structure ou qu'ils fassent partie des intervenants et correspondants habituels de celle-ci. Elle précise les objectifs poursuivis et l'organisation mise en œuvre pour les atteindre, en affectant des moyens dédiés et/ou en mutualisant certaines fonctions.

2.1.2 Quels sont les objectifs poursuivis ?

La politique d'identitovigilance a pour objectif de définir la stratégie organisationnelle la plus adaptée pour :

- favoriser le respect des bonnes pratiques d'identification par tous les acteurs (professionnels et usagers) ;
- garantir la confiance dans la qualité des informations échangées entre les professionnels de santé internes et les correspondants externes (établissements de santé, structures médico-sociales, prestataires…) ;
- s'assurer de l'interopérabilité entre les systèmes d'information en santé ;
- sécuriser le rapprochement d'identités (applications internes, systèmes d'information des partenaires, applications régionales, services nationaux comme le dossier médical partagé (DMP)…) ;
- identifier, analyser et prévenir les anomalies en lien avec des erreurs d'identification des usagers pris en charge.

2.1.3 Quel est son périmètre d'application ?

La politique d'identitovigilance s'applique à tous les modes de prise en charge assurés par la structure : hébergement, consultation, soins à domicile, actes de télémédecine, etc.

Les acteurs concernés sont :

- l'usager, acteur de sa sécurité, et ses accompagnants : ayant-droit, personne de confiance, représentant légal ;
- les professionnels de santé ou du secteur médico-social concourant à la prise en charge.

De façon non exhaustive, ces professionnels sont :

- les médecins, pharmaciens, dentistes, sages-femmes ;
- les paramédicaux (infirmiers, aides-soignants, psychologues, kinésithérapeutes…) ;
- les assistantes médicales, médico-administratives et médico-sociales ;
- les ambulanciers et brancardiers ;
- les personnels des services médicotechniques (laboratoire, imagerie, pharmacie, services mortuaires…) ;
- les travailleurs sociaux ;
- les agents administratifs participant à l'identification des usagers ;
- les intervenants d'organisation tierces réalisant des prises de rendez-vous par téléphone ou par voie électronique ;
- les industriels développant les solutions informatiques utilisées par la structure…

2.1.4 Comment communiquer autour de cette politique ?

Il est important que la politique menée pour améliorer la qualité de prise en charge et la sécurité des usagers fasse l'objet d'une large communication à tous les niveaux afin de généraliser l'acculturation souhaitée. Elle doit être aussi bien menée :

- en interne, par l'intermédiaire des professionnels impliqués dans les démarches qualité et gestion des risques ;
- en externe, en informant régulièrement les parties prenantes sur les objectifs, les moyens et les résultats.

2.2 Gouvernance de l'identitovigilance

La structuration des moyens de pilotage (gouvernance) et de mise en œuvre opérationnelle est à adapter aux ressources humaines disponibles dans la structure – ou le groupe auquel elle appartient – et à l'évaluation des risques associés à son activité et à la population accueillie. Elle repose classiquement sur plusieurs niveaux :

- une instance stratégique ;
- une instance opérationnelle pilotée par un référent identitovigilance ;
- une instance consultative.

Du fait de ressources réduites, un grand nombre de SNH peuvent se contenter de mettre en place une seule instance. Elle peut être dédiée à l'identitovigilance ou s'intégrer dans une démarche de coordination de la gestion des risques (GDR).

Remarque : le document utilise le terme « instance de pilotage » pour nommer cette instance unique.

Toute structure non hospitalière doit se doter d'instance(s) de gouvernance dédiées à la gestion des risques adaptée(s) à sa taille et à ses activités. [Exi SNH 01]

Remarque : pour les structures plus importantes, et les groupements de SNH, il est recommandé de se calquer sur les préconisations faites aux établissements de santé (cf. § 2.2 RNIV 2).

2.2.1 Quelles sont les préconisations relatives à l'instance de pilotage ?

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 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 (ou équivalent) ;
- le référent en identitovigilance de la structure ;
- le responsable du système d'information (ou équivalent) ;
- le responsable de la sécurité des systèmes d'information (RSSI ou équivalent le cas échéant) ;
- le délégué à la protection des données quand la structure en est dotée ;
- des représentants des professionnels de la structure.

Dans la mesure du possible, et si cela est pertinent au regard de l'activité de la structure, il peut être associé :
- des référents en identitovigilance de structures partenaires (pharmacie, laboratoire, imagerie, établissement de santé…) ;
- un représentant d'usagers.

2.2.1.3 Fonctionnement

La composition, les objectifs et les modalités de fonctionnement de l'instance sont précisés dans un règlement intérieur. Chaque réunion, dont la fréquence est déterminée en fonction des besoins, donne lieu à la rédaction d'un compte rendu de réunion ou d'un relevé d'informations-décisions-actions (RIDA).

2.2.2 Quelles sont les préconisations relatives au référent en identitovigilance ?

Un référent en identitovigilance doit être identifié dans toute structure de santé de plus de 10 professionnels. [Exi SNH 02]

Les missions spécifiques du référent en identitovigilance, en plus de ses fonctions habituelles, sont de :
- participer à l'instance de pilotage ;
- promouvoir les bonnes pratiques d'identitovigilance en interne, conformément aux exigences règlementaires et aux recommandations nationales et régionales applicables ;
- former les professionnels de la structure ;
- représenter la SNH au sein du réseau régional des référents en identitovigilance ;
- alerter le responsable ou le coordonnateur de la structure sur les difficultés rencontrées et les risques relatifs à l'identitovigilance.

2.3 Évaluation de la politique

Il est nécessaire que l'instance de pilotage mette en place des outils permettant d'évaluer l'efficacité et l'efficience de la stratégie et des actions arrêtées de façon à pouvoir les faire évoluer. Il est recommandé de définir :

- des modalités de suivi des actions (exemples : respect des échéances du plan d'actions) ;
- des indicateurs de structure (exemples : cohérence du système d'information avec les règles opposables ; existence d'un système de signalement adapté à l'identification des erreurs d'identification ; organisation facilitant la conduite effective des actions préventives et correctives…)
- des indicateurs de processus (exemples : évaluation du respect des bonnes pratiques d'identification secondaire par la réalisation d'audits ciblés…) ;
- des indicateurs de résultats (exemples : suivi de l'évolution de la fréquence des erreurs d'identification associées aux soins ; typologie et gravité des événements indésirables liés à ces erreurs…).

2.4 Documentation

2.4.1 Quelles sont les règles générales à appliquer ?

La structure doit veiller à mettre à jour les documents qualité pour prendre en compte sans délai les préconisations et règles établies :

- au niveau national, déclinées soit par voie réglementaire (décret, arrêté, instruction…) soit par l'intermédiaire de documents rendus opposables : référentiels, chartes, guides de bonne pratique ;
- au niveau régional voire territorial, complétant les précédentes pour favoriser le déploiement des bonnes pratiques ou s'adapter à des particularités locales : politique régionale, modèles de documents qualité, fiches pratiques, guides…

Tous les documents relatifs à la sécurisation de l'identification ont vocation à être réunis dans un *manuel qualité* dédié à l'identitovigilance : chartes et référentiels, documents qualité et procédures locales…

2.4.2 Que doit contenir la charte d'identitovigilance ?

La charte d'identitovigilance (cf. Exi PP 15 RNIV 1) a pour objet de rappeler les principes à respecter pour :

- recueillir l'identité des usagers en respectant les préconisations en vigueur ;
- prévenir les risques liés à une mauvaise identification ;
- harmoniser les pratiques et favoriser l'acculturation des professionnels en termes de sécurité ;
- impliquer les usagers dans cette exigence de sécurité.

Cette charte comprend obligatoirement les informations suivantes :

- la politique et la gouvernance mises en œuvre dans la structure (engagement dans la sécurité, y compris celle du système d'information, structuration, membres…) ;

- la description du système d'information dédié à l'identification des usagers, de ses modalités de sécurisation et, si applicable, des interfaces (cartographie applicative) ;
- les modalités d'attribution des habilitations pour la gestion des identités numériques ;
- les solutions d'identification primaire et secondaire de l'usager en vigueur dans la structure ;
- la gestion documentaire associée à l'identification des usagers et à la gestion des risques (cf. 2.4.4) ;
- la liste des indicateurs suivis (cf. 2.5) ;
- les références réglementaires et techniques applicables…

Elle doit aussi rappeler les droits de l'usager d'être informé en cas de traitement automatisé des informations les concernant, de l'ensemble des droits qui lui sont reconnus au titre du RGPD et des modalités pratiques d'exercice de ces droits (accès aux informations médicales le concernant, possibilité de demander la rectification, voire la suppression, de données erronées ou obsolètes, notamment). Pour rappel, l'établissement doit également procéder à un affichage de ces mentions d'informations à l'attention des usagers, conformément aux exigences posées par l'article 13 du RGPD, laquelle devra notamment préciser que l'INS des usagers est collecté et traité.

2.4.3 Quelles sont les procédures opérationnelles à formaliser ?

En fonction de ses activités et de l'évaluation des risques, un certain nombre de procédures opérationnelles doivent être formalisées et mises en application par toutes les parties prenantes. Par exemples :

- Identification primaire lors de l'accueil de l'usager dans la structure ;
- Identification secondaire d'un usager avant tout acte de soin ;
- Signalement des événements indésirables relatifs à l'identification d'un usager ;
- Utilisation d'un bracelet d'identification, si applicable ;
- 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 ;
- Information des partenaires après détection d'une erreur d'identification ;
- Contrôle qualité des identités numériques et gestion des erreurs ;
- Modification d'une identité numérique ;
- Etc.

2.4.4 Quels sont les autres documents opérationnels à détenir ?

2.4.4.1 Charte d'utilisation du système d'information de santé

Lorsque la SNH utilise un système d'information partagé gérant des données de santé à caractère personnel, elle doit formaliser une charte informatique qui énonce les règles d'accès et d'usage de cet outil (cf. Exi PP 13 RNIV 1). Elle précise notamment la politique d'habilitation et les droits individuels attribués aux professionnels ainsi que les modalités d'enregistrement des accès aux dossiers et des modifications effectuées.

Elle est diffusée aux professionnels présents ainsi qu'aux nouveaux arrivants et, si c'est pertinent, aux prestataires et sous-traitants.

2.4.4.2 Cartographie des flux applicatifs

Lorsque la SNH utilise plusieurs applications informatiques partageant des données de santé, les interfaces d'identité entre ces différents outils doivent être décrites dans un document qualité : la cartographie des flux applicatifs (cf. Exi PP 12 RNIV 1). Cette dernière précise les interfaces mises en œuvre entre le référentiel d'identités (cf. 3.2.2.1) et les autres applications utilisant les identités numériques (champs échangés, relation maître-esclave, types d'interfaces…).

Il est recommandé que les interfaces respectent le cadre d'interopérabilité (CI-SIS) qui garantit la transmission exhaustive des informations afférentes à l'identité numérique.

2.5 Indicateurs qualité

Les indicateurs qualité ont pour but d'évaluer la performance du système. Il est important d'en disposer à la fois sur les pratiques d'identification primaire que secondaire.

Pour exemples (non exhaustifs) :
- Proportions d'identités qualifiées, validées, récupérées, provisoires (cf. § 3.3.1 RNIV 1) ;
- Taux de doublons de flux (calculé sur la file active) ;
- Taux d'identités possédant le même matricule INS ;
- Taux de signalements d'événements indésirables relatifs à l'identification primaire des usagers ;
- Taux de signalements d'événements indésirables relatifs à l'identification secondaire des usagers ;
- Taux de formation des professionnels de la structure à l'identitovigilance, par catégorie professionnelle…

3 Gestion des risques

3.1 Principes généraux

3.1.1 Quels sont les enjeux ?

La GDR, indissociable de la démarche d'amélioration continue de la qualité, est particulièrement importante en identitovigilance. Elle a pour objet d'identifier les lieux, professionnels et situations qui sont associés à des risques d'erreurs d'identification afin de mettre en place des *barrières de sécurité* destinées à diminuer la probabilité de survenue des erreurs. Elle est classiquement distinguée en 2 approches complémentaires selon le moment où l'action est menée.

La GDR *a priori* est focalisée sur la prévention des risques évitables. Elle consiste à identifier les menaces, à les analyser en termes de probabilité de survenue et de gravité potentielle des conséquences afin de déterminer les mesures barrières susceptibles de les éviter et la priorité de leur mise en œuvre effective (cf. 3.1.3).

La GDR *a posteriori* est destinée à détecter et analyser les dysfonctionnements. Elle repose sur la déclaration des événements indésirables (EI) et l'organisation d'un retour d'expérience (REX) qui associe une analyse des facteurs ayant abouti à l'erreur et la mise en œuvre d'un plan d'actions correctrices et/ou préventives (cf. 3.1.4).

3.1.2 Sur qui repose l'organisation de la GDR en identitovigilance ?

La qualité et la sécurité des données personnelles des usagers, enregistrées dans le système d'information, doivent être l'une des priorités du responsable (ou du coordonnateur) de la SNH. Elle doit être l'une des missions principales confiées au référent en identitovigilance de la structure.

3.1.3 Comment élaborer la cartographie des risques *a priori* ?

3.1.3.1 Objectif

La GDR *a priori* a pour objet d'identifier les risques potentiels de mauvaise identification des usagers dans la structure. Les dysfonctionnements prévisibles sont colligés dans une « cartographie des risques » et associés à des informations qui permettent de les classer :

- par catégorie d'erreur (lieu, situation, type…) ;
- par criticité (produit de la fréquence prévisible et du score de gravité des conséquences effectives ou potentielles sur la sécurité de l'usager).

Elle facilite la prise de décision en termes d'actions préventives à mettre en place (*barrières de prévention*) et de priorités d'intervention.

3.1.3.2 Organisation

Pour établir la cartographie des risques liés aux erreurs d'identification, il est nécessaire de réunir un panel représentatif des professionnels de la structure afin de balayer les situations problématiques pouvant être rencontrées dans les différentes activités de la structure, de recenser les moyens existant pour les maîtriser et d'anticiper les mesures barrières supplémentaires à mettre en place.

Cette analyse des risques *a priori* doit idéalement être réalisée par une *approche processus* qui permet de mettre en évidence les dysfonctionnements potentiels aux interfaces entre activités. Il est particulièrement important d'identifier les circonstances de prise en charge qui présentent un risque plus élevé d'erreurs d'identification que la moyenne (niveau de criticité élevé, moyen ou faible) et où une attention toute particulière doit être portée à l'identitovigilance, en termes de respect de bonnes pratiques, de formation et de sensibilisation des professionnels et des usagers.

Les risques sont souvent plus élevés, par exemple, pour certains usagers (incapables de décliner leur identité ou de participer à la sécurité de leur prise en charge, en difficulté sociale…) et certaines pratiques (le circuit du médicament).

3.1.3.3 Exemples de risques a priori dans un SNH

<table>
<tr><th>Types d'erreurs</th><th>Par qui, où, quand ?</th><th>Conséquences possibles</th></tr>
<tr><td>Erreur de saisie des traits d'identité</td><td>Professionnels assurant l'accueil des usagers</td><td>Création inappropriée d'un nouveau dossier (doublon) ou utilisation d'un mauvais dossier (collision)</td></tr>
<tr><td>Défaut de vérification avant un acte, interprétation incorrecte de l'identité</td><td rowspan="2">Tous professionnels soignants, brancardiers, prestataires…</td><td>Erreur de personne pour la réalisation d'un acte technique</td></tr>
<tr><td>Erreur de dossier, d'usager, d'étiquetage</td><td>Mauvaise attribution des résultats
Erreur de diagnostic
Retard de prise en charge</td></tr>
</table>

Utilisation frauduleuse d'identité	Usager	Mélange de données (collision) appartenant à plusieurs usagers dans un même dossier Décision erronée du professionnel sur la base de mauvaises informations

3.1.3.4 Exemples de barrières de sécurité

Typologie des risques de dysfonctionnements	*Actions préventives*
Saisie des traits d'identité lors de l'accueil de l'usager	Procédure d'accueil administratif, formation des agents, organisation d'un contrôle de cohérence *a posteriori…*
Sélection du dossier dans lequel sont enregistrées des informations de santé	Procédure d'identitovigilance, sensibilisation en staffs de service, outils de communication…
Réalisation de gestes techniques chez un usager	
Remise de documents de coordination des soins	Procédure de sortie des usagers, formation des professionnels concernés…
Connaissance des procédures	Audit des connaissances et des pratiques, formation initiale et continue…
Utilisation frauduleuse d'identité	Information et sensibilisation de l'usager aux risques encourus Modalités de dépistage par les professionnels

3.1.4 Comment identifier les risques *a posteriori* ?

3.1.4.1 Objectifs

La GDR *a posteriori* a pour objet d'identifier et d'analyser les événements indésirables (EI) liés à une mauvaise identification des usagers dans la structure. Elle repose sur le signalement de ces EI et sur l'organisation de retours d'expériences (REX).

3.1.4.2 Organisation

3.1.4.2.1 Signalement des EI

Les anomalies en rapport avec l'identification primaire ou secondaire – potentielles et avérées – doivent être déclarées au sein du système de signalement des événements indésirables (SSEI) interne à la structure.

La procédure doit permettre :

- de catégoriser les EI en fonction des conséquences (exemples : erreur d'administration d'un traitement, réalisation inappropriée d'un examen, mauvaise identification d'un document…) ;
- d'évaluer la criticité de l'EI (produit de la fréquence et de la gravité), que les conséquences soient potentielles (événement porteur de risque) ou avérées (dommages constatés).

Il est important que le système d'information, papier ou numérique, permette la catégorisation des EI avec des attributs multiples (exemple : erreur médicamenteuse + erreur d'identitovigilance) afin de pouvoir identifier ceux qui sont liées à des erreurs d'identification et de produire des statistiques pertinentes qui seront mises à disposition de l'instance de pilotage.

Les EI en rapport avec l'identitovigilance peuvent aussi faire l'objet :

- d'une déclaration externe, sur le portail national de signalement des événements sanitaires indésirables[1], au titre des obligations réglementaires en vigueur relatives aux vigilances et aux événements indésirables graves associés aux soins (EIGS) ;
- d'un signalement aux autorités compétentes pour les ESMS[2] ;
- d'une procédure d'alerte des parties prenantes lorsque l'événement a permis la propagation d'une identité erronée (cf. 3.2.2.3).

Il est également de bonne pratique de partager (en interne à la structure voire en externe, au niveau territorial et/ou régional) les informations relatives à des erreurs inhabituelles d'identification primaires ou secondaires rencontrées afin de permettre au plus grand nombre de mettre en place les barrières de sécurité adéquates.

3.1.4.2.2 Organisation de retours d'expériences

La GDR en rapport avec les EI signalés est réalisée dans le cadre de l'organisation de REX qui comprennent systématiquement :

- une analyse des facteurs institutionnels, organisationnels et humains ayant conduit à l'erreur ;
- la mise en œuvre d'actions correctives et/ou préventives à mettre en œuvre dans les meilleurs délais pour éviter que l'EI ne se reproduise ou en minimiser les conséquences potentielles, en fonction des priorités déterminées par la structure et de ses moyens.

Selon la politique et l'organisation de l'identitovigilance de la structure, les REX doivent être organisés systématiquement ou ciblés sur certains EI : les plus graves, les plus récurrents, les plus critiques, ceux qui sont porteurs des risques les plus importants…

Les REX doivent être réalisés selon une méthode validée par la Haute Autorité de santé (HAS)[3] :

- pour les événements indésirables répétitifs de même type, sans conséquence grave (événements porteurs de risques, EPR), il est recommandé de mettre en place un *comité de retour d'expérience* (CREX) dédié aux erreurs d'identitovigilance. Une équipe réduite « d'experts », accompagnées par le référent en identitovigilance, est chargée d'enquêter sur les facteurs favorisant les dysfonctionnements et de faire des propositions qui seront ensuite discutées en séance élargie avec les professionnels concernés ;
- pour les erreurs à l'origine d'un EIGS, il est nécessaire d'utiliser une méthodologie d'adaptée (exemples : REMED pour les EI liés aux médicaments, ALARM(E) pour les autres), dans le cadre d'une analyse approfondie des causes (AAC) isolée ou intégrée dans une revue de morbi-mortalité (RMM). Un appui méthodologique peut être demandé à la structure régionale d'appui (SRA) à la qualité et à la sécurité.

Les REX font systématiquement l'objet de comptes rendus anonymisés qui sont transmis à l'instance de pilotage.

3.1.4.3 Exemples d'événements indésirables

Événements indésirables	*Conséquences*
Prescriptions réalisées dans le mauvais dossier	

[1] https ://signalement.social-sante.gouv.fr/

[2] Art. L. 331-8-1 du Code de l'action sociale et des familles

[3] Cf. la synthèse de la *Prévention Médicale* (https ://www.prevention-medicale.org/Dossiers-du-risque-et-methodes-de-prevention/Methodes-de-prevention/Structures-favorisant-le-retour-d-experience/analyse-evenement-grave-rmm-crex-remed)

Administration d'un traitement au mauvais patient/résident	Traitements inappropriés chez les 2 patients concernés, iatrogénie
Rangement d'un compte-rendu dans le dossier d'un autre usager	Attribution d'antécédents incorrects au patient, erreurs sur le traitement à mettre en place, retard diagnostique…
Erreur de validation d'une identité	Envoi inapproprié de données avec un matricule INS
Utilisation frauduleuse d'identité	Collisions entre les données de santé de 2 usagers

3.1.4.4 Exemples de barrières de sécurité

Typologie des dysfonctionnements	*Actions correctives*
Erreur d'identification primaire	Améliorer la procédure d'accueil, sensibiliser les agents, mettre en place des contrôles de cohérence *a posteriori…*
Erreur d'identification secondaire	Réaliser une évaluation des pratiques, proposer des actions de type *patient traceur…*
Remise ou envoi de documents de coordination des soins	Formaliser la procédure de sortie des usagers, former et sensibiliser les professionnels concernés…

3.2 Sécurisation des démarches d'identification primaire

3.2.1 Quelles sont les règles générales à appliquer ?

L'identification primaire comprend l'ensemble des opérations destinées à attribuer une identité numérique à un usager physique qu'il s'agisse d'une première prise de contact avec l'usager ou d'une venue ultérieure. Elle recouvre les étapes de recherche, de création, de modification d'une identité ainsi que l'attribution d'un niveau de confiance aux données enregistrées (cf. § 3.3.2 RNIV 1).

En termes d'identification primaire, les barrières de sécurité reposent sur (liste indicative) :
- le respect des règles opposables (RNIV, recommandations régionales, procédures territoriales et/ou locales) ;
- l'évaluation des acquis des professionnels après les actions de formation et de sensibilisation ;
- la mise en place de conditions favorables au respect des bonnes pratiques, notamment par le professionnel récemment arrivé qu'il faut veiller à ne pas mettre en difficulté ;
- la sensibilisation et l'information des usagers qui doivent être acteurs de leur parcours de soin, chaque fois que possible ;
- la déclaration systématique des anomalies détectées secondairement au système de signalement des événements indésirables (cf. 3.1.4.2.1)…

Il est rappelé en outre qu'il est interdit de pratiquer des « validations automatiques » des identités numériques au bout d'un certain délai, sans passer par l'étape obligatoire de contrôle de cohérence des traits de l'identité numérique avec ceux portés sur un dispositif d'identité à haut niveau de confiance (cf. Exi PP 08 RNIV 1).

3.2.2 Comment sécuriser l'utilisation des identités numériques ?

3.2.2.1 Référentiel d'identité

Lorsqu'elle emploie plusieurs logiciels métiers, la structure doit disposer d'un référentiel unique d'identités (cf. Exi SI 13 RNIV 1). C'est un ensemble de composants (techniques et organisationnels) du système d'information qui garantit la cohérence des données d'identité pour l'ensemble des logiciels gérant des informations nominatives des usagers pris en charge.

3.2.2.2 Prévention des collisions

Une collision correspond à l'utilisation d'une même identité numérique pour au moins 2 personnes physiques différentes. Elle est liée à 3 sources d'erreurs :

- l'enregistrement de données dans un mauvais dossier (informatique ou papier) ;
- l'utilisation frauduleuse de l'identité d'un usager déjà enregistré localement ;
- une opération de fusion réalisée à tort entre des dossiers n'appartenant pas au même usager.

Elle fait courir le risque de prendre des décisions de prise en charge au regard des données de santé d'une autre personne et peut être très difficile à corriger pour faire la part, *a posteriori*, des informations médicales qui relèvent de chaque usager.

Il est donc important que la structure définisse clairement les moyens de prévention à mettre en œuvre, essentiels dans ce type d'événement indésirable. Ils passent par :

- la formation et la sensibilisation régulière des acteurs ;
- l'information des usagers sur l'attention qu'ils doivent apporter à leur identification, en tant qu'acteurs de leur sécurité ;
- la mise en œuvre de procédures d'accueil visant à dépister autant que faire se peut une utilisation frauduleuse d'identité lorsque ce type de situation est observée dans la structure.

Le dépistage et le signalement des anomalies au moindre doute fait partie des bonnes pratiques collectives. Ils favorisent la mise en route d'actions correctrices sans perte de temps. La structure doit définir et formaliser les procédures permettant d'identifier et de corriger ces événements indésirables potentiellement graves.

3.2.2.3 Propagation des modifications d'identité

3.2.2.3.1 Utilisation de protocoles d'interopérabilité

Lorsque les structures partagent des flux d'information d'identité en utilisant des protocoles d'interopérabilité conformes ou non au CI-SIS, du standard IHE PAM ou d'autres types d'interfaces, la propagation des modifications d'identité numérique aux autres domaines d'identification concernés doit, de préférence, être réalisée automatiquement par ce biais.

Les cas d'usage nécessitant une intervention humaine doivent être préalablement identifiés dans la cartographie des flux applicatifs. (cf. 2.4.4.2). Un dispositif d'alerte spécifique aux structures concernées doit alors être mis en œuvre (cf. 3.2.2.3.2).

3.2.2.3.2 En l'absence d'interface informatique entre structures concernées

La structure doit réaliser une analyse d'impact pour connaître les correspondants auxquels l'identité initiale a été transmise et les risques associés.

La propagation des modifications d'identité aux correspondants externes concernés[4] doit, en priorité, concerner celles qui portent sur les traits stricts : correction d'une erreur de saisie, changement de sexe, erreur d'attribution de l'INS, incident de type collision, envoi d'un courrier avec identité erronée…

Faute de pouvoir être réalisée de façon automatique lorsqu'il s'agit d'une erreur portant sur les traits stricts (message de correction IHE PAM), elle doit faire l'objet d'une information écrite (courrier postal, messagerie sécurisée) aux correspondants en précisant les modifications apportées.

Dans le cas du dossier médical partagé (DMP), le professionnel qui a publié un document erroné a la possibilité de le supprimer et de le remplacer par une version corrigée.

En fonction de l'urgence et de la gravité potentielle de l'erreur, l'information écrite pourra être doublée par une information orale.

Dans tous les cas :
- la structure doit veiller à garder un historique des transmissions réalisées ;
- les erreurs doivent être déclarées dans le système de signalement des événements indésirables et faire l'objet d'un retour d'expérience **(cf. 3.1.4.2).**

3.2.2.4 Contrôle qualité de la base d'identités numériques et gestion des anomalies

La structure doit régulièrement contrôler la qualité des identités numériques du référentiel d'identité, notamment à la recherche de doublons, d'identités incohérentes (par exemples : âge >120 ans, sexe incohérent avec le prénom).

La réalisation de la fusion de dossiers en doublons sous une même identité numérique n'est autorisée que pour des personnels spécialement formés et habilités, sous le contrôle du référent en identitovigilance de la structure. Le système d'information doit garder une trace des modifications effectuées (cf. Exi SI 14 RNIV 1).

3.2.3 Comment sécuriser l'enregistrement de l'identité numérique locale ?

3.2.3.1 Modification d'une identité numérique

La modification d'une identité numérique n'est autorisée que pour des personnels habilités de la structure **(cf. 2.4.4.1)** qui doivent être en nombre limité. Elle est décrite dans une procédure interne spécifique **(cf. 2.4.3).**

Elle ne peut être réalisée qu'au vu d'un document d'identité officiel, conformément à la procédure du recueil de l'identité. Le système d'information doit garder une trace des modifications effectuées (cf. Exi SI 14 RNIV 1).

Après que la modification a été enregistrée, il faut s'assurer que l'information est transmise à tous les acteurs concernés **(cf. 3.2.2.3)** et que chaque pièce du dossier comporte bien la nouvelle identité **(cf. 3.3.3.1).**

---

[4] Article 19 du Règlement général de protection des données (RGPD) : https ://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article19

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

3.2.3.2 Contrôle qualité de la saisie manuelle des traits d'identité

Lors de la création ou de la modification manuelle d'une identité numérique, il est recommandé de mettre en place des mécanismes de contrôle de la qualité de la saisie (cf. § 3.3.3 RNIV 1). Après avoir vérifié la cohérence des données enregistrées par comparaison à une pièce d'identité officielle on peut ajouter d'autres éléments de contrôle comme, par exemple :

- demander à l'usager (ou à son accompagnant) d'énoncer à voix haute ses principaux traits d'identification et/ou de vérifier l'exactitude des informations qui le concernent en faisant relire à l'usager les traits imprimés ou visualisés à l'écran ;
- faire contrôler *a posteriori* la cohérence des données de l'identité numérique par une autre personne avec les traits portés par le document d'identité enregistré[5].

3.2.4 Comment sécuriser l'utilisation de l'identité INS ?

3.2.4.1 Erreur d'attribution d'une identité INS à un usager

Ce type d'erreur peut potentiellement se produire dans les cas :

- de la sélection d'un mauvais bénéficiaire lors de l'interrogation du téléservice par l'intermédiaire de la carte Vitale ;
- d'un mauvais contrôle de cohérence à la réception des données renvoyées par le téléservice (cf. Annexe VI RNIV 1).

Lors du constat de l'erreur d'attribution d'une identité INS, la structure doit informer l'ensemble des professionnels avec lesquels il a partagé des données en utilisant ce mauvais identifiant. La conduite à tenir est précisée au § 3.2.2.3).

3.2.4.2 Constat d'un écart avec une identité numérique au statut Identité qualifiée

Le statut *Identité qualifié* correspond au plus haut niveau de confiance pouvant être attribué à une identification. Il est donc réputé stable dans le temps mais des modifications de l'état civil restent possibles, ce qui justifie l'opération de vérification tous les 3 à 5 ans préconisée par le référentiel INS.

Il existe toutefois des situations où la qualification de l'identité peut, malgré tout le soin apporté à l'opération, s'avérer erronée ou suspecte. C'est le cas, par exemple, lors de la découverte d'une utilisation frauduleuse de l'identité d'un autre usager ou lorsqu'une opération de vérification par appel du téléservice INSi révèle, *a posteriori*, des écarts inattendus.

Cette absence de cohérence est problématique et doit faire l'objet d'une enquête spécifique. En attendant de connaître les raisons de cette incohérence, l'enregistrement peut faire l'objet, sur décision des professionnels concernés, d'un déclassement en *Identité provisoire* (cf. § 2.3.1 ainsi que Annexes VI et VII du RNIV 1).

[5] Sous réserve du respect des règles de conservation des données en vigueur.

3.2.5 Comment sécuriser la gestion des identités approchantes ?

Il est important de définir comment identifier et gérer les identités numériques qui peuvent facilement être confondues entre elles lorsqu'elles présentent des traits aux caractéristiques proches. Cette situation augmente le risque d'erreur :

- lors de la création ou de la modification de l'identité numérique (risque de collision) ;
- lors de la prise en charge (risque de collision par erreur de dossier, d'étiquette…) ;
- lors des opérations de traitement des doublons (fusion inadéquate de dossiers).

Ces identités approchantes concernent :

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

Remarque : l'utilisation du matricule INS pour les identités *récupérées* et *qualifiées* doit permettre d'éviter la fusion accidentelle entre 2 dossiers n'ayant pas le même identifiant mais ne protège en rien de l'erreur de sélection de dossier.

Il appartient aux acteurs et structures concernés de mettre en place des garde-fous pour éviter le risque de collision accidentelle des données par erreur de choix de dossier entre 2 identités numériques approchantes dans les opération administratives et soignantes. Il est conseillé de formaliser une procédure qui décrit :

- comment faire la liste des identités numériques concernées ;
- dans quelles conditions utiliser l'attribut *Identité* h*omonyme* – qui n'est pas réservé aux seuls homonymes vrais (cf. § 2.3.2 RNIV 1) – et comment assurer sa transmission dans les logiciels tiers ;
- quel type d'affichage mettre en place pour alerter les professionnels lorsqu'ils recherchent et sélectionnent une de ces identités approchantes (attribut homonyme en clair ou codé, couleur spécifique, signes distinctifs, etc.) ;
- comment signaler une erreur rattrapée (événement porteur de risque) en lien avec ce type de situation…

3.3 Sécurisation des démarches d'identification secondaire

3.3.1 Quelles sont les règles générales à appliquer ?

L'identification secondaire consiste à s'assurer systématiquement de la cohérence entre l'identité de l'usager physique et l'identité portée sur la prescription / le document / le dossier / le geste technique qui le concerne(nt). Il s'agit de vérifier que l'usager bénéficiaire de l'acte est bien celui pour lequel l'acte a été prescrit.

Les barrières mises en place dans ce domaine sont à définir par la structure, selon des critères qui dépendent :

- de la probabilité pour le professionnel de reconnaître l'usager sans risque d'erreur (prise en charge individuelle ou dans un établissement d'hébergement, ancienneté de la relation entre l'usager et le professionnel…) ;
- de la possibilité de faire participer l'usager à sa sécurité (adhésion, compréhension…) ;
- des dispositifs d'identification pouvant être utilisés dans la structure.

3.3.2 Comment sécuriser l'identification de l'usager ?

3.3.2.1 Identification orale

La façon la plus simple de s'assurer de l'identification d'un usager communiquant avant la réalisation d'un soin est de lui demander de décliner son identité par le biais de questions ouvertes. Les usagers doivent être sensibilisés à l'importance de cette méthode qui est essentielle à leur sécurité.

3.3.2.2 Dispositifs d'identification physique

Plusieurs dispositifs peuvent participer à l'identification des usagers dans les structures réalisant des hébergements tels que : la pose d'un bracelet, l'utilisation d'une photographie dans son dossier[6], l'affichage sur les portes de chambres des résidents, etc. L'usage d'un dispositif d'identification et les personnes à qui il doit être proposé font partie des décisions attendues de l'instance de pilotage.

Son utilisation doit faire l'objet d'une procédure qui décrit :
- l'information de l'usager, de sa famille ou de sa personne de confiance ;
- les modalités de préparation, de pose et dépose du bracelet ou de mise à jour de la photographie ;
- les modalités pratiques d'utilisation ;
- la conduite à tenir en cas de refus de ce type d'identification ou de nécessité de dépose du bracelet en cours de séjour, quelle qu'en soit la raison…

Il faut éviter la transcription manuelle de l'identité de l'usager sur le bracelet (source d'erreurs) et privilégier les bracelets comportant une identité imprimée à partir des données informatisées (cf. § 3.4.1 RNIV 1).

3.3.3 Comment sécuriser l'utilisation des documents de prise en charge ?

3.3.3.1 Identification des informations relatives à l'usager

Les SNH doivent veiller à ce que tous les documents liés à la prise en charge d'un usager (courrier, prescription, demande d'examen, document de transfert…) soient identifiés correctement (cf. Exi PP 10 RNIV 1). Il est important de vérifier qu'aucune équivoque n'est possible sur la nature des traits, notamment dans les échanges entres structures différentes (cf. Exi SI 11 RNIV 1).

3.3.3.2 Cohérence entre documents

À chaque étape de sa prise en charge, la cohérence de l'identité de l'usager (déclinée ou relevée sur le dispositif d'authentification physique) et celle relevée sur les documents (prescription, pilulier, étiquette, comptes rendus…) doit être contrôlée.

De même, la cohérence entre 2 documents (prescription et étiquettes pour identification des prélèvements par exemple) doit être vérifiée.

---

[6] Sous réserve du respect du droit à l'image et de la réglementation applicable

Remarque : les couples mariés doivent faire l'objet d'une attention particulière en cas de séjour simultané dans la structure. Il en est de même pour les personnes ayant des identités approchantes (cf. 3.2.5).

3.4 Formation et sensibilisation à l'identitovigilance

3.4.1 Qu'est-ce que la notion de culture de sécurité partagée ?

Le respect des règles d'identification repose sur leur compréhension et leur appropriation par toutes les parties prenantes : professionnels comme usagers.

Cette culture de sécurité partagée autorise notamment :
- la mise en œuvre de barrières de sécurité comprises par tous, en routine ;
- le signalement des événements indésirables sans crainte de sanction.

3.4.2 Comment améliorer la culture de sécurité des parties prenantes ?

3.4.2.1 Formation des professionnels

La formation et la sensibilisation des professionnels à l'identitovigilance doit faire partie des actions du plan de formation annuel de toute structure non hospitalière. [Exi SNH 03]

La formation et la sensibilisation de l'ensemble des professionnels doivent être prévues par la SNH. Elles peuvent être dédiées à un seul volet de l'identification (primaire ou secondaire) en fonction des objectifs attendus et de la population concernée et, chaque fois que possible, associer les correspondants externes : ambulanciers, professionnels et structures adressant des usagers, plateaux techniques…

Des évaluations régulières, par contrôle de connaissance ou audit de pratique, peuvent être organisées en fonction des besoins afin de s'assurer que les professionnels :
- partagent un bon niveau de culture de sécurité dans le domaine de l'identification ;
- maîtrisent les applicatifs qu'ils utilisent ;
- savent appliquer les procédures, y compris les fonctionnements en mode dégradé…

3.4.2.2 Information et sensibilisation des usagers

Une attention toute particulière doit être portée à la communication réalisée auprès des usagers et de leur famille (affichage, livret d'accueil, explications orales…), qui doit leur permettre de connaître leurs droits et de comprendre l'importance de l'identitovigilance. Ils doivent être incités à participer à leur bonne identification primaire et secondaire.

L'usager ne peut s'opposer à l'utilisation de son identité INS mais doit en être informé[7]. Cette information doit être partagée dans les instances où siègent des représentants d'usagers, dont le Conseil de la vie sociale (CVS) pour les structures médico-sociales.

[7] Cf. Référentiel INS

ANNEXE I - Exigences et recommandations applicables

Exigences et recommandations spécifiques aux SNH

Exi SNH 01	Toute structure non hospitalière doit se doter d'instance(s) de gouvernance dédiées à la gestion des risques adaptée(s) à sa taille et à ses activités.
Exi SNH 02	Un référent en identitovigilance doit être identifié dans toute structure de santé de plus de 10 professionnels.
Exi SNH 03	La formation et la sensibilisation des professionnels à l'identitovigilance doit faire partie des actions du plan de formation annuel de toute structure non hospitalière.
Reco SNH 01	La politique d'identitovigilance doit être intégrée à la politique qualité et sécurité conduite par la structure – ou par le groupe auquel elle appartient.

Exigences et recommandations communes relatives au système d'information (RNIV 1)

Exi SI 01	Le système d'information doit permettre, *a minima*, d'effectuer la recherche d'une identité numérique à partir : - de tout ou partie de l'identité INS récupérée après l'interrogation du téléservice INSi ; - de la saisie de la date de naissance, éventuellement complétée par les premiers caractères du nom ou du prénom.
Exi SI 02	L'utilisation du matricule INS pour la recherche d'antériorité doit être sécurisée pour éviter tout risque lié à une erreur de saisie. Si le matricule n'est pas récupéré électroniquement, la saisie des 15 caractères du NIR et leur validation par la clé de contrôle est obligatoire pour toute recherche à partir du matricule INS.
Exi SI 03	Lors de la recherche d'un usager dans la base d'identités, il est nécessaire que le système d'information interroge sans distinction, avec les données correspondantes mais sans tenir compte des tirets ou apostrophes, les champs *Nom de naissance* et *Nom utilisé*, ainsi que les champs *Prénom(s) de naissance*, *Premier prénom de naissance* et *Prénom utilisé*.
Exi SI 04	Les traits d'identification doivent faire l'objet de champs spécifiques dans le système d'information.
Exi SI 05	Le système d'information doit obligatoirement proposer 3 champs dédiés à l'enregistrement des traits complémentaires suivants : Premier prénom de naissance, Nom utilisé et Prénom utilisé.
Exi SI 06	Les informations récupérées du téléservice INSi font l'objet d'un stockage et d'une traçabilité au niveau du système d'information de santé.
Exi SI 07	Tout système d'information en santé doit permettre d'attribuer un des 4 statuts de confiance à chaque identité numérique stockée.
Exi SI 08	Le système d'information doit garantir que seul le statut *Identité qualifiée* permette le référencement des données de santé échangées avec le matricule INS, en conformité avec la réglementation applicable.
Exi SI 09	Pour les identités numériques comportant un attribut Identité douteuse ou Identité fictive, il doit être informatiquement rendu impossible :

	- d'attribuer un statut autre que celui d'*Identité provisoire* ; - de faire appel au téléservice INSi.
Exi SI 10	Le type de dispositif d'identité ayant servi au recueil de l'identité doit être enregistré. Seul un document à haut niveau de confiance, ou son équivalent numérique, doit autoriser l'attribution des statuts *Identité validée* ou *Identité qualifiée*.
Exi SI 11	Il est important que la nature de chaque trait d'identité affiché sur les documents et les interfaces homme machine soit facilement reconnue, sans risque d'équivoque, par tous les acteurs de santé concernés.
Exi SI 12	Après attribution du statut *Identité qualifiée* ou *Identité récupérée*, les traits INS doivent remplacer, si ce n'est pas déjà le cas, les traits stricts locaux dans les champs correspondants.
Exi SI 13	Les structures doivent disposer d'un référentiel unique d'identités assurant la cohérence des données pour l'ensemble des logiciels gérant des informations nominatives des usagers.
Exi SI 14	Il est indispensable que les accès et les modifications apportées aux identités soient tracés (date, heure, type de modification et professionnel ayant réalisé l'action). Les récupérations successives de l'INS doivent également être enregistrées.
Exi SI 15	Les systèmes d'information peuvent permettent de traduire dans le format JJ/MM/AAA les dates de naissance libellées dans un calendrier luni-solaire pour les usagers nés à l'étranger.
Reco SI 01	Il est recommandé que les systèmes d'information en santé autorisent l'emploi d'attributs supplémentaires pour permettre aux professionnels de caractériser les identités numériques nécessitant un traitement particulier.
Reco SI 02	Il est recommandé que le système d'information dispose de fonctionnalités dédiées à la recherche des anomalies portant sur l'enregistrement des traits d'identité.

Exigences communes relatives aux pratiques professionnelles (RNIV 1)

Exi PP 01	L'appel au téléservice INSi est obligatoire pour vérifier une identité INS reçue lorsque l'identité numérique n'existe pas ou qu'elle ne dispose pas d'un statut récupéré ou qualifié.
Exi PP 02	La création d'une identité numérique requiert la saisie d'une information dans au moins 5 traits stricts : nom de naissance, premier prénom de naissance, date de naissance, sexe et lieu de naissance.
Exi PP 03	Les champs relatifs à la liste des prénoms de naissance et au matricule INS sont renseignés dès qu'il est possible d'accéder à ces informations : présentation d'un titre d'identité et/ou appel au téléservice INSi, dans les cas d'usage où l'emploi du matricule INS est requis et autorisé.
Exi PP 04	Il est nécessaire de renseigner le maximum de traits complémentaires, selon les consignes que chaque structure définit en fonction de ses besoins.
Exi PP 05	Avant toute intégration de l'identité INS dans l'identité numérique locale, il est nécessaire de valider la cohérence entre les traits INS renvoyés par le téléservice INSi et les traits de la personne physique prise en charge.

Exi PP 06	L'interrogation du téléservice INSi par l'intermédiaire de la carte vitale est le mode d'interrogation à privilégier chaque fois que possible.
Exi PP 07	L'attribution d'un niveau de confiance à toute identité numérique est obligatoire.
Exi PP 08	Afin d'utiliser une identité numérique de confiance, il est indispensable de s'assurer, *a minima* lors du premier contact physique de l'usager dans une structure, que les justificatifs d'identité présentés correspondent bien à la personne prise en charge.
Exi PP 09	Il est formellement interdit de procéder à la validation d'une identité numérique sans pouvoir contrôler sa cohérence à la lumière d'un titre d'identité à haut niveau de confiance, ou son équivalent numérique, dont le type est dument enregistré dans le système d'information.
Exi PP 10	Il doit être affiché *a minima* les traits stricts suivants : nom de naissance, premier prénom de naissance, date de naissance, sexe et, sur les documents comportant des données d'information de santé, le matricule INS suivi de sa nature (NIR ou NIA) lorsque cette information est disponible et que son partage est autorisé.
Exi PP 11	Dès lors que son identité est passée au statut *Identité qualifiée*, le matricule INS et les traits INS doivent être utilisés pour l'identification de l'usager, notamment lors des échanges de données de santé le concernant.
Exi PP 12	Les structures doivent disposer d'une cartographie applicative détaillant en particulier les flux relatifs aux identités. Les outils non interfacés nécessitant une intervention humaine pour mettre à jour les identités doivent être identifiés.
Exi PP 13	Une charte informatique formalisant les règles d'accès et d'usage du système d'information, et en particulier pour les applications gérant des données de santé à caractère personnel, doit être élaborée au sein de chaque structure à exercice collectif.
Exi PP 14	Les acteurs de santé impactés par la diffusion d'une erreur en lien avec l'identité INS doivent être alertés sans délai, selon une procédure spécifique formalisée par la structure.
Exi PP 15	Les structures de santé d'exercice collectif doivent formaliser la politique institutionnelle d'identification de l'usager au sein d'une charte d'identitovigilance.
Exi PP 16	Comme pour les autres traits stricts, la date de naissance à enregistrer est celle établie d'après un document ou un dispositif officiel d'identité et non celle lue sur un document de l'Assurance maladie, qui peut être différente.
Exi PP 17	L'enregistrement du *nom utilisé* est obligatoire lorsqu'il est différent du *nom de naissance*.
Exi PP 18	L'enregistrement du *prénom utilisé* est obligatoire lorsqu'il est différent du *premier prénom de naissance*.
Reco PP 01	Pour obtenir des résultats pertinents, il est fortement recommandé de limiter le nombre de caractères saisis pour effectuer la recherche d'un enregistrement.
Reco PP 02	Il est important que toute difficulté rencontrée pour la récupération de l'identité INS ou la qualification de l'identité numérique, du fait d'une

	incohérence non mineure, soient signalée comme événement indésirable et rapportée au niveau régional et national.

Les exigences posées par le RNIV viennent en compléments de celle posées par le référentiel INS.

ANNEXE II – Glossaire

AAC : Analyse approfondie des causes d'événements indésirables
ALARM(E) : *Association of Litigation And Risk Management (Extended)*, technique d'AAC
ARS : Agence régionale de santé
CDS : Centre de santé
CI-SIS : Cadre d'interopérabilité des systèmes d'information en santé
CPTS : Communauté professionnelle territoriale de santé
CREX : Comité de retour d'expérience
DAC : Dispositif d'appui à la coordination
DMP : Dossier Médical Partagé
EI : Événement indésirable
EIGS : Événement indésirable grave associé aux soins
EPR : Événement porteur de risques
ESP : Équipe de soins primaires
Exi : Exigences rendues opposables par le RNIV
GDR : Gestion des risques
IHE PAM : *Integrating the Healthcare Enterprise Patient Administration Management* (utilisation coordonnée de standards d'interopérabilité pour les échanges informatisés de données de santé)
INS : Identité Nationale de Santé
INSi : Téléservice de recherche et de vérification de l'identité nationale de santé (INS)
MSP : Maison de santé pluriprofessionnelle
Reco : Recommandation du RNIV
REX : Retour d'expérience
RGPD : Règlement général de protection des données
RMM : Revue de morbi-mortalité
RNIV 1 : Référentiel national d'identitovigilance. Partie 1 (Document socle)
RNIV 2 : Référentiel national d'identitovigilance. Partie 2 (Identitovigilance en établissement de santé)
ROR : Répertoire Opérationnel des Ressources
SCM : Société civile de moyens
SNH : Structures non hospitalières
SIS : Système d'information en santé
SRA : Structure régionale d'appui à la qualité et la sécurité des soins
SSEI : Système de signalement des événements indésirables
USLD : Unité de soins de longue durée

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

Liberté
Égalité
Fraternité