

Référentiel National d'identitovigilance

IDENTITOVIGILANCE EN
ETABLISSEMENT DE SANTE Volet 2

SOMMAIRE

1	INTRODUCTION	1
1.1	Objet du document.....	1
1.2	Structures concernées.....	1
1.3	Rappel des enjeux.....	1
1.4	Périmètre de l'identitovigilance.....	2
2	POLITIQUE ET GOUVERNANCE	2
2.1	Politique d'identitovigilance.....	2
2.1.1	Formalisation de la politique d'identitovigilance.....	2
2.1.2	Objectifs poursuivis.....	2
2.1.3	Périmètre d'application.....	3
2.1.4	Communication autour de cette politique.....	3
2.2	Gouvernance de l'identitovigilance.....	4
2.2.1	Préconisations relatives à l'instance stratégique.....	4
2.2.2	Préconisations relatives à l'instance opérationnelle.....	5
2.2.3	Préconisations relatives au référent en identitovigilance.....	7
2.2.4	Préconisations relatives à l'instance consultative.....	8
2.3	Évaluation de la politique.....	8
2.4	Organisation de la gestion des identités numériques	8
2.5	Documentation.....	9
2.5.1	Règles générales à appliquer.....	9
2.5.2	Charte d'identitovigilance.....	9
2.5.3	Les procédures opérationnelles à formaliser.....	10
2.5.4	Autres documents opérationnels.....	11
2.6	Indicateurs qualité.....	13
3	GESTION DES RISQUES	13
3.1	Principes généraux.....	13
3.1.1	Enjeux.....	13
3.1.2	Organisation de la GDR en identitovigilance.....	14
3.1.3	Elaborer la cartographie des risques <i>a priori</i>	14
3.1.4	Identifier les risques <i>a posteriori</i>	17
3.2	Sécurisation des démarches d'identification primaire.....	19
3.2.1	Règles générales à appliquer.....	19
3.2.2	Sécuriser l'utilisation des identités.....	20
3.2.3	Sécuriser l'enregistrement de l'identité locale.....	22
3.2.4	Sécuriser l'utilisation de l'INS.....	23
3.2.5	Sécuriser la gestion des identités approchantes.....	24
3.2.6	Gérer une suspicion d'utilisation frauduleuse d'identité.....	25
3.3	Sécurisation des démarches d'identification secondaire.....	26
3.3.1	Règles générales à appliquer.....	26
3.3.2	Sécuriser l'identification de l'utilisateur.....	26
3.3.3	Sécuriser l'utilisation des documents de prise en charge.....	27

3.4	Formation et sensibilisation à l'identitovigilance	28
3.4.1	Notion de culture de sécurité partagée	28
3.4.2	Améliorer la culture de sécurité des parties prenantes.....	28
ANNEXE I - EXIGENCES ET RECOMMANDATIONS APPLICABLES.....		I
ANNEXE II – GLOSSAIRE DES SIGLES UTILISES		X
ANNEXE III EXEMPLES D'ORGANISATION DE GESTION DES IDENTITES		XII

REDACTEURS

Mme Céline DESCAMPS, GRADeS Nouvelle Aquitaine (ESEA)

M. Thierry DUBREU, GRADeS Ile de France (SESAN)

Mme Soizick GOUY, GRADeS Pays de la Loire (GCS e-santé)

M. Jean-Baptiste MILONE, DNS

Dr Manuela OLIVER, GRADeS Provence-Alpes-Côte d'Azur (ieSS), Service de Santé des Armées

Mme Emilie PASSEMARD, DNS

M. Bertrand PINEAU, GRADeS Ile de France (SESAN)

M. Geoffroy SINEGRE, DNS

RELECTEURS

M. Bruno CHAMPION, DGS

Dr Gilles HEBBRECHT, DGOS

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

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	30/10/2020	1 ^{ère} mise en ligne du document
1.1	20/12/2020	Correction de coquilles et ajustements mineurs de contenu
1.2	20/05/2021	Mise à jour, notamment suite avis CNIL
2.0	13/12/2024	Mise à jour

Guide de lecture

Les modifications par rapport à la précédente version sont surlignées **en bleu clair** (lorsque les modifications portent sur un paragraphe complet, seul le titre du paragraphe est surligné) :

- de nouvelles exigences ont été ajoutées, d'autres supprimées ;
- certaines recommandations ont été passées en exigences ;
- des exigences initialement présentes dans le RNIV1 ont été déplacées vers les RNIV 2 et/ou 3 ;
- le plan a été modifié ;
- certaines annexes ont été intégrées dans le corps du texte.

Le choix a été fait de :

- conserver la numérotation initiale des exigences et recommandations et de numéroter à la suite les nouvelles exigences ;
- ne pas réutiliser les numéros attribués précédemment aux exigences ou recommandations supprimées.

Par conséquent, les exigences n'apparaissent plus par ordre chronologique dans le texte.

1 Introduction

1.1 Objet du document

Le présent document vise à préciser les recommandations et bonnes pratiques applicables aux Etablissements de santé – ou aux groupements de ce type de structures– en matière d’identification des usagers, en complément des règles et recommandations éditées dans le document socle du Référentiel national d’identitovigilance (RNIV 1).

Il est annexé au référentiel « Identité nationale de santé », qu’il vient compléter.

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

Convention sémantique : Pour faciliter la lecture, le terme « identité » sera systématiquement employé pour désigner l’identité numérique de l’usager dans un système d’information.

1.2 Structures concernées

Les structures concernées dans ce document sont les établissements de santé publics et privés.

Les agences régionales de santé (ARS), sur avis éventuel de l’instance stratégique régionale d’identitovigilance peuvent toutefois décider :

- que certains établissements de santé, du fait de leur taille réduite ou du faible turnover de leurs patients (exemples : USLD, SMR, certaines unités de psychiatrie, unités de dialyse), relèvent plutôt des mesures simplifiées développées dans le 3^e volet (RNIV 3) dédié aux « structures non hospitalières » ;
- de rendre *a contrario* le volet 2 applicable à certaines structures non hospitalières, 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).

Remarque : certaines « structures non hospitalières » peuvent choisir volontairement de conduire une politique qualité plus exigeante en appliquant les préconisations du RNIV 2.

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 ou le mode de prise en charge (médecine, obstétrique, chirurgie, hospitalisation à domicile, rééducation, soins ambulatoires, télésoins et télésanté, etc.) 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 par un établissement ou un professionnel de santé pour fiabiliser et sécuriser l'identification de l'utilisateur à toutes les étapes de sa prise en charge. Elle concerne :

- l'élaboration de documents de bonnes pratiques relatifs à l'identification de l'utilisateur ;
- 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 la prise en charge de l'utilisateur en termes :

- *d'identification primaire* qui vise à attribuer une identité unique à chaque usager dans le système d'information 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.

2 Politique et gouvernance

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

2.1 Politique d'identitovigilance

2.1.1 Formalisation de la politique d'identitovigilance

L'établissement de santé formalise une politique d'identitovigilance en accord avec la politique qualité et sécurité conduite par la structure ou par le groupe auquel il appartient. [RECO ES 07]

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 Objectifs poursuivis

La politique d'identitovigilance a pour objectif de définir la stratégie organisationnelle qui semble 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 avec les correspondants externes (médecins traitants, sous-traitants, etc.) ;
- s'assurer de l'interopérabilité entre les systèmes d'information en santé (SIS) ;

- sécuriser le rapprochement d'identités (applications internes, systèmes d'information des partenaires, applications régionales, services nationaux comme le dossier médical partagé (DMP), etc.) ;
- identifier, analyser et prévenir les anomalies en lien avec des erreurs d'identification des usagers pris en charge.

2.1.3 Périmètre d'application

La politique d'identitovigilance s'applique à tous les modes de prise en charge assurés par la structure : hospitalisation complète ou partielle, consultation, hospitalisation et soins à domicile, actes de télésanté, etc.

Les acteurs concernés sont :

- l'utilisateur, acteur de sa sécurité, et ses accompagnants : ouvrant droit, personne de confiance, représentant légal ;
- les professionnels de santé assurant la prise en charge ;
- les autres professionnels qui interviennent sur tout ou partie des données médico-socio-administratives des usagers.

De façon non exhaustive, ces professionnels sont :

- les médecins, pharmaciens, dentistes, sage-femmes ;
- les paramédicaux (infirmiers, aides-soignants, psychologues, kinésithérapeutes, auxiliaires de puériculture, etc.) ;
- les assistants médicaux, médico-administratifs et médico-sociaux ;
- les ambulanciers et brancardiers ;
- les personnels des services médicotecniques (laboratoire, imagerie, pharmacie, services mortuaires, etc.) ;
- les travailleurs sociaux ;
- les agents administratifs réalisant l'identification d'usagers ou traitant les données de santé (bureau des entrées, service des archives, département d'information médicale, plateau technique, service informatique, etc.) ;
- les intervenants de sociétés tierces réalisant des prises de rendez-vous par téléphone ou par voie électronique ;
- etc.

2.1.4 Communication 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 équipes dédiées à la qualité et à la gestion des risques généraux et/ou spécifique à l'identitovigilance ;
- 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 la mise en œuvre opérationnelle est à adapter aux ressources humaines disponibles dans la structure, 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 en identitovigilance ;
- une instance consultative.

Des instances stratégique et opérationnelle dédiées à l'identitovigilance doivent être mises en place par les établissements de santé et les groupements de structures. [EXI ES 01]

2.2.1 Préconisations relatives à l'instance stratégique

2.2.1.1 Missions

Cette instance décisionnaire est chargée (liste indicative) de :

- participer à la définition de la politique d'identitovigilance et de formation des acteurs dans ce domaine ;
- arrêter l'organisation à mettre en œuvre (structuration des instances, missions qui leur sont confiées) ;
- définir les moyens humains, techniques et financiers à attribuer pour le fonctionnement optimal de cette organisation ;
- valider le plan annuel ou pluriannuel d'actions à conduire ;
- effectuer un suivi des actions et de leurs résultats en s'appuyant sur des indicateurs pertinents ;
- décider des actions correctives à mettre en œuvre ;
- communiquer sur la politique et ses résultats.

Remarque : pour les établissements faisant partie d'un groupement hospitalier de territoire (GHT) ou d'un groupe d'établissements privés, l'instance stratégique peut être celle du niveau de décision le plus élevé.

2.2.1.2 Composition

La composition de cette instance stratégique dépend de la taille et de l'activité de l'établissement – ou du groupe de structures. Les membres sont désignés par le responsable de la structure et de la Commission (ou conférence) médicale d'établissement (CME).

La composition recommandée est la suivante, par fonctions (responsable en titre ou représenté), à adapter au niveau de l'instance (territoriale ou locale) :

- le directeur de l'établissement ;
- le président de la commission médicale d'établissement ;
- le directeur des soins (ou équivalent) ;
- le médecin responsable du département d'information médicale (DIM) (ou équivalent) ;
- le responsable des admissions ;
- le référent en identitovigilance de la structure ;
- le responsable des systèmes d'information ;
- le responsable de la sécurité des systèmes d'information (RSSI) ;
- le responsable qualité gestion des risques de l'établissement ;

- le coordonnateur de la gestion des risques associés aux soins ;
- le délégué à la protection des données de l'établissement.

Dans la mesure du possible, et si cela est pertinent au regard de l'activité de la structure, il est conseillé d'associer :

- un représentant de chacun des domaines « satellites » (pharmacie, imagerie, laboratoire, bloc opératoire, etc.) ;
- le référent en identitovigilance des structures partenaires ;
- le correspondant local en hémovigilance et sécurité transfusionnelle ;
- un représentant du service des archives ;
- un représentant des 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 donne lieu à la rédaction d'un compte rendu de réunion ou relevé de décision et d'action.

La fréquence des réunions est à déterminer en fonction des besoins mais est au moins semestrielle pour les établissements de santé.

2.2.2 Préconisations relatives à l'instance opérationnelle

2.2.2.1 Missions

Dans les établissements de santé, la cellule opérationnelle est le plus souvent dénommée *Cellule d'identitovigilance* (CIV). Son rôle est de rester en contact avec l'ensemble des acteurs afin de participer à l'amélioration continue des pratiques et de la culture de sécurité dans ce domaine.

Cette instance est chargée de piloter ou de participer aux réflexions et aux actions relatives à l'identitovigilance (liste indicative), en lien avec les responsables concernés, et notamment de :

- participer à la formation des professionnels, dans le cadre du plan de formation de la structure, y compris lors de l'accueil des nouveaux arrivants, toutes catégories de professionnels confondues ;
- initier et mener des actions de sensibilisation des usagers et des partenaires externes ;
- analyser les risques *a priori* (cartographie des risques), y compris les risques liés à la sécurité informatique ;
- formaliser et/ou actualiser les documents qualité relatifs à l'identitovigilance ;
- prendre part aux retours d'expériences des événements indésirables en lien avec des erreurs d'identification ;
- définir, suivre et analyser les indicateurs relatifs à l'identitovigilance ;
- réaliser des audits de connaissance et de pratiques ;
- guider les professionnels sur la conduite à tenir vis-à-vis des cas particuliers ;
- contrôler la qualité des identités dans les domaines d'identification utilisés par la structure ;
- réaliser le traitement des anomalies signalées (doublons, collisions, **cas complexes de qualification de l'INS, etc.**) ;
- contribuer au rapprochement d'identités entre structures pour les identités des usagers qui ne disposent pas d'INS ;
- réaliser la veille réglementaire et technique, etc.

Elle rend compte à l'instance stratégique des actions conduites et des difficultés rencontrées.

Remarque : pour les établissements faisant partie d'un groupement hospitalier de territoire (GHT) ou d'un groupe d'établissements privés, les différentes instances opérationnelles locales peuvent s'associer pour réaliser des missions communes ou des évaluations croisées.

2.2.2.2 Composition

Les professionnels composant la CIV, identifiés pour leurs compétences en identitovigilance, sont désignés par le responsable de la structure et placés sous l'autorité technique du référent en identitovigilance de la structure (cf. § 2.2.3). Il peut s'agir de personnels médicaux, paramédicaux, administratifs, médico-administratifs, etc.

Leur nombre est défini en fonction des missions confiées et des activités de la structure. Des préconisations en équivalents temps plein (ETP) annuels sont données dans le tableau suivant. Ces préconisations sont adaptables selon la taille et la typologie d'activités.

Activités	Structure de court séjour sans accueil d'urgence ni accueil délocalisé	Structure avec service(s) ayant une charge de travail particulière (accueil délocalisé, urgences, etc.)	Structure de moyen et long séjour (SMR, USLD, etc.)
Pilotage de la vigilance, organisation, suivi et analyse des indicateurs (dont le temps du référent identitovigilance), etc.	0,2 ETP < 500 lits/places 0,5 ETP 500> et <1000 lits/places 1 ETP >1000 lits/places		0,1 ETP pour la structure
Gestion de la (des) bases(s) d'identités, dont traitement des anomalies (doublons, collisions), rapprochement, etc.	0,05 ETP/10 000 identités*	0,10 ETP/10 000 identités*	
Actions de formation et de sensibilisation	0,1 ETP/200 personnels		0,1 ETP pour la structure
Réalisation d'audits de pratique	0,03 ETP/200 personnels		
Qualification des identités en back office	0,15 ETP/10 000 identités**		

* identités : nombre d'utilisateurs différents pris en charge dans la structure annuellement.

** le temps dédié nécessaire évalué ici correspond à la phase de peuplement des bases identité par des identités INS qualifiées. Cette charge ira en diminuant avec le temps.

Ces préconisations sont données à titre indicatif. Elles sont généralistes et ne peuvent prendre en compte toutes les particularités. Chaque structure évalue le nombre d'équivalents temps plein (ETP) nécessaire à cette fonction en prenant en compte différents facteurs qui doivent être évalués à l'échelle de la structure ou du groupement, selon le cas :

- taille de la structure et activité (file active, nombre de séjours, pratiques d'activités à risque, etc.) ;

- modalités de fonctionnement de la structure (présence ou non de personnels dédiés assurant directement l'accueil administratif dans les unités accueillant des usagers, y compris en heure de permanence des soins, tels que les services d'urgence, maternité, consultations, etc.) ;
- particularités en termes de population prise en charge (fréquence des suspicions de fraudes d'identité, des procédures d'accueil relevant de l'anonymat, par exemple) ;
- accueil administratif des usagers organisé en différents sites délocalisés ou utilisant une application autre que l'outil maître des identités pour réaliser l'identification du patient ;
- participation ou non à un partage d'identités.

2.2.2.3 Fonctionnement

La composition, les objectifs et les modalités de fonctionnement de la CIV sont précisés dans un règlement intérieur. Chaque réunion donne lieu à la rédaction d'un compte rendu de réunion ou d'un relevé d'informations-décisions-actions (RIDA).

Par définition, la CIV doit assurer un fonctionnement quotidien, au moins pendant les heures ouvrables.

2.2.3 Préconisations relatives au référent en identitovigilance

Un référent en identitovigilance doit être identifié dans tout établissement de santé. [EXI ES 02]

Chaque structure de santé désigne au moins un référent en identitovigilance. Il est membre de la CIV et de l'instance stratégique. Il est nommé par la direction de la structure, en concertation avec le président de la CME, sur proposition de cette dernière instance. Il dispose d'une fiche de poste et d'un temps dédié à cette activité.

En fonction de la taille, du nombre d'implantations géographiques de la structure et/ou de particularités organisationnelles, il peut être décidé de nommer plusieurs référents locaux, avec une subordination technique à l'un d'entre eux qui exerce cette fonction au titre de l'entité juridique.

Les missions du référent en identitovigilance, en plus de ses fonctions habituelles, sont (à titre indicatif) de :

- promouvoir les bonnes pratiques d'identitovigilance conformément, aux exigences règlementaires et aux recommandations nationales et régionales applicables ;
- piloter la cellule opérationnelle afin qu'elle réponde aux besoins des parties prenantes ;
- représenter la structure dans l'instance consultative régionale d'identitovigilance ;
- participer à la gestion des risques liés aux erreurs d'identification et à la coordination des vigilances ;
- alerter le responsable de la structure sur les difficultés rencontrées en matière de lutte contre les risques relatifs à l'identitovigilance.

Le référent en identitovigilance est identifié :

- au niveau de la structure ;
- dans l'observatoire des systèmes d'information en santé (oSIS) de la plateforme ATIH ;
- auprès du référent régional en identitovigilance¹ **[EXI ES 05]**

¹ [Liste des référents régionaux en identitovigilance](#)

Remarque : la fonction de référent en identitovigilance peut être exercée au niveau d'un groupement hospitalier de territoire (GHT) ou d'un groupe d'établissements privés ; cette fonction se cumule avec celle de référent local.

2.2.4 Préconisations relatives à l'instance consultative

Il n'est pas obligatoire de mettre en place une instance consultative au niveau de la structure ; cela relève de la décision de l'instance stratégique correspondante. Si cela est le cas, elle doit être constituée de représentants des différentes catégories professionnelles impliquées dans les questions d'identification afin de donner un avis sur la politique, la formation ou les documents qualité qui leur sont soumis :

- membres de CIV ;
- référents métiers logiciels ;
- représentants des parties prenantes (professionnels de santé, médico-sociaux, usagers, sous-traitants, responsables/référents systèmes d'information, etc.).

Remarque : il peut être décidé de mettre en place une instance consultative au niveau du groupement hospitalier de territoire (GHT) ou du groupe d'établissements privés en faisant notamment appel à des représentants des différentes instances opérationnelles et/ou stratégiques des structures qui la composent.

2.3 Évaluation de la politique

Il est bien entendu nécessaire de mettre en place des outils permettant d'évaluer l'efficacité, l'efficience de la stratégie et des actions arrêtées de façon à pouvoir les faire évoluer. Il est recommandé que chaque instance définisse :

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

Un bilan périodique, au moins annuel, doit être transmis aux instances décisionnelles en précisant, par exemple :

- le nombre et le type de réunions ;
- le nombre et la nature des incidents relevés ;
- les résultats des indicateurs suivis ;
- les corrections et améliorations conduites.

2.4 Organisation de la gestion des identités numériques

La structure de santé doit organiser la gestion des identités : création, modification, fusion des identités, interrogation du téléservice INSi, qualification de l'INS et gestion des cas complexes (discordances entre

les traits de l'INS et les traits présents sur un dispositif d'identification à haut niveau de confiance, réponse « aucune identité trouvée » ou « plusieurs identités trouvées » du téléservice INSi, erreur d'attribution d'une INS, etc.).

La gestion des anomalies et des cas complexes nécessite des professionnels formés, dédiés à l'identitovigilance et la mise en place d'une organisation spécifique. Celle-ci est dépendante du flux quotidien d'utilisateurs, de la file active de la structure, de l'activité et de l'organisation de l'établissement (accueil en urgences, maternité, point d'accueil délocalisé, etc.), de la typologie de personnes prises en charge (précarité sociale, utilisateurs nés à l'étranger, utilisateurs âgés, etc.). Il est préconisé de disposer d'une organisation comportant deux niveaux :

- un premier niveau (front office) constitué par les professionnels accueillant l'utilisateur qui peuvent effectuer l'appel au téléservice INSi, la qualification des identités dans les cas simples ;
- un second niveau (le back-office), chargé du contrôle qualité, de l'étude des cas complexes, de la qualification des identités des utilisateurs accueillis en heures de permanence des soins, de la gestion des anomalies, etc.

L'ANNEXE III Exemples d'organisation de gestion des identités décrit plusieurs types d'organisation possibles.

2.5 Documentation

2.5.1 Règles générales à appliquer

L'établissement 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 ministérielle, etc.), soit par l'intermédiaire de documents rendus opposables : référentiels, chartes, guides de bonne pratique ;
- au niveau régional, 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, etc.

Tous les documents relatifs à la sécurisation de l'identification des utilisateurs ont vocation à être présents dans la gestion documentaire de l'établissement : chartes et référentiels, documents qualité et procédures locales, etc.

2.5.2 Charte d'identitovigilance

Les structures de santé d'exercice collectif doivent formaliser la politique institutionnelle d'identification de l'utilisateur au sein d'une charte d'identitovigilance. [EXI PP 15]

La charte d'identitovigilance peut être commune à plusieurs structures associées. Elle a pour objet de rappeler les principes à respecter pour :

- recueillir l'identité des utilisateurs en respectant les préconisations en vigueur ;
- prévenir les risques liés à une mauvaise identification ;
- harmoniser les pratiques et favoriser l'acculturation à la sécurité des professionnels ;
- impliquer les utilisateurs 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, instances, membres des instances, etc.) ;
- la description des systèmes d'informations participant à l'identification primaire de l'utilisateur et des interfaces (cartographie applicative) ;
- la liste des points de création d'identités de la structure ;
- les modalités d'attribution des habilitations pour la gestion des identités ;
- les solutions d'identification primaire et secondaire de l'utilisateur en vigueur dans la structure (bracelet d'identification, photographie², contrôle de cohérence de l'identité de l'utilisateur avant un acte de soin, etc.) ;
- la gestion documentaire associée à l'identification des usagers et à la gestion des risques (procédures, modes opératoires, etc.) ;
- la liste des indicateurs suivis ;
- les références réglementaires et techniques applicables, etc.

Elle doit aussi rappeler les droits de l'utilisateur 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 collectée et traitée.

2.5.3 Les procédures opérationnelles à formaliser

En fonction de la taille de la structure de santé, des types de prises en charge réalisées et des risques identifiés, un certain nombre de procédures opérationnelles doivent être formalisées et mises en application par toutes les parties prenantes.

Exemples :

- identification primaire lors de l'accueil de l'utilisateur dans la structure (à détailler par lieux assurant cet accueil) ;
- identification secondaire d'un usager avant tout acte de soin ;
- recherche d'un dossier d'utilisateur dans la base de données de la structure ;
- signalement des événements indésirables relatifs à l'identification ;
- information des partenaires après détection d'une erreur d'identification d'un usager ;
- correction d'une identité ;
- identification d'un nouveau-né ou d'un enfant à naître, avec les liens mère-enfant ;
- enregistrement d'un usager incapable de donner ou justifier son identité ;
- identification des usagers placés sous main de justice ;
- identification des usagers présentant des troubles psychiatriques ;
- identification des victimes lors de situation sanitaire exceptionnelle (afflux massif) ;
- admission d'un usager souhaitant garder l'anonymat ou ne souhaitant pas divulguer sa présence dans l'établissement ;

² Sous réserve du respect du droit à l'image et des règles de conservation des données en vigueur

- gestion des cas réglementaires d'anonymat (accouchement dans le secret, cure de désintoxication, etc.) ;
- utilisation d'un bracelet d'identification ;
- gestion des rapprochements d'identités ;
- gestion des doublons et fusions d'identités ;
- gestion des collisions ;
- gestion d'une suspicion de substitution frauduleuse d'identité ;
- gestion des identités dans les logiciels non ou incomplètement interfacés, appartenant à des domaines d'identification différents ou non ;
- gestion des homonymes et des identités approchantes ;
- contrôle qualité des bases d'identités ;
- contrôle de la sécurité du système d'information ;
- 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 ;
- gestion des patients tests ;
- gestion des transferts entre établissements ;
- gestion d'une INS erronée (correction, information des parties prenantes en interne et en externe) ;
- gestion de la suppression des pièces d'identités stockées ;
- etc.

2.5.4 Autres documents opérationnels

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

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 l'établissement. [EXI PP 13].

Validée par le niveau stratégique d'identitovigilance de la structure, elle formalise notamment la politique d'habilitation et les droits individuels attribués aux professionnels (cf. § 2.5.4.3) ainsi que les modalités d'enregistrement des accès aux dossiers et des modifications effectuées.

Elle doit être régulièrement actualisée et diffusée aux professionnels présents ainsi qu'aux nouveaux arrivants et, si cela est pertinent, aux prestataires et sous-traitants.

2.5.4.2 Cartographie des flux applicatifs

Les interfaces d'identités entre les outils participant à l'identification de l'utilisateur doivent être décrites dans un document qualité : la cartographie des flux applicatifs (cf. RNIV 1 [EXI PP 12]). Cette dernière précise les interfaces mises en œuvre entre le référentiel d'identités (cf. § 3.2.2.1) et les autres applications utilisant des identités (champs échangés, relation maître-esclave, types d'interfaces, etc.).

Il est recommandé que les interfaces respectent le cadre d'interopérabilité (CI-SIS) qui garantit la transmission exhaustive des informations afférentes à l'identité. Les standards d'échanges sont développés dans des documentations spécifiques.

2.5.4.3 Habilitations

Les habilitations décrites dans la charte d'utilisation du SIS (cf. § 2.5.4.1) concernent plusieurs niveaux différents qu'il convient de distinguer.

2.5.4.3.1 Droits d'accès

Il est rappelé aux professionnels ayant accès aux données confidentielles du système d'information qu'ils sont soumis à une obligation de confidentialité (secret professionnel).

L'accès au dossier de l'utilisateur, qu'il soit numérique (réseau et logiciels) ou physique (papier), est strictement limité aux professionnels qui contribuent à assurer sa prise en charge (notion de cercle de soins et protocoles de coopération) ou qui ont des droits réglementaires spécifiques (exemples : médecin DIM, professionnels recueillant les indicateurs qualité et sécurité des soins, comités de retour d'expérience, etc.).

Il est nécessaire de mettre en place des précautions particulières lorsqu'un professionnel accède à des données d'un patient qu'il ne prend pas directement en charge, notamment dans le cadre de l'urgence (procédure « bris de glace ») et de l'accès des services de veille sanitaire des ARS à des données devant donner lieu à un signalement de maladie à déclaration obligatoire (MDO). [RECO ES 01]

2.5.4.3.2 Droits de création, modification d'identité et d'interrogation du téléservice INSi

Les droits de création et de modification d'identité et d'interrogation du téléservice INSi dans le système d'information doivent être réservés à un nombre limité de professionnels spécifiquement formés. Ils sont nommément désignés par le responsable de la structure, en cohérence avec la politique d'habilitation des personnes autorisées à créer ou valider l'identité d'un usager : bureau des entrées, services assurant un accueil direct, secrétariat médical, etc.

2.5.4.3.3 Droits de rapprochement et de fusion

La possibilité de réaliser le rapprochement et/ou la fusion entre 2 dossiers ne doit être attribuée qu'à des professionnels spécialement désignés. Des dispositions complémentaires sont prises pour assurer la propagation de la fusion dans les logiciels tiers lorsque la propagation des modifications ne peut pas être réalisée automatiquement (cf. § 3.2.2.3).

2.5.4.3.4 Rôle des référents logiciels

Un référent (au moins) doit être nommé pour chaque logiciel métier participant à la prise en charge de l'utilisateur. Il est l'interlocuteur privilégié du référent en identitévigilance de la structure pour tout ce qui concerne l'identité de l'utilisateur. Il détient des droits spécifiques, déterminés par la structure, en fonction de ses missions.

Le référent logiciel s'assure que l'outil répond aux exigences de la charte d'identitévigilance de la structure (cf. § 2.5.2). Si l'outil fait partie d'un autre domaine d'identification, il participe aux tests d'interface d'identité et aux contrôles de cohérence entre le référentiel d'identité de l'outil et le référentiel d'identités maître de la structure. Il met en œuvre les actions nécessaires à la gestion de la base d'identités de l'outil (report de fusion ou de modifications d'identité si l'outil est incomplètement interfacé par exemple). Partie prenante de la gestion des risques, il est associé à l'évaluation des risques *a priori* et, si besoin, à l'analyse des événements indésirables.

2.6 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 et secondaire.

La HAS met en œuvre des indicateurs nationaux qualité et sécurité des soins (IQSS) intégrant des attendus sur l'identification du patient ; ils sont rendus annuellement sur la plateforme QUALHAS³. Des indicateurs opérationnels d'identitovigilance sont à développer – au niveau national, régional ou local – avec une priorité à donner à ceux identifiés par un astérisque (*) dans la liste ci-dessous. Leurs modalités de calcul sont précisées dans des cartes d'identités d'indicateurs⁴. Ils peuvent être inscrits dans les contrats pluriannuels d'objectifs et de moyens (CPOM) des établissements par l'ARS et faire l'objet de comparaisons inter établissements.

Exemples (non exhaustifs) :

- taux de doublons de flux* (calculé sur la file active) ;
- nombre de collisions détectées* ;
- nombre de fusions ;
- rapport entre doublons avérés dans la file active et fusions réalisées, permettant d'apprécier la charge de travail des cellules d'identitovigilance et l'adéquation des ressources avec les besoins* ;
- délai moyen de traitement d'un doublon potentiel (par classe : en 24 h ; une semaine ; un mois ; plus long) ;
- taux de modifications d'identités par type de traits ;
- proportions d'identités qualifiées, validées, récupérées, provisoires* ;
- nombre de suspicions d'utilisation frauduleuse d'identité détectées ;
- 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* ;
- nombre/Taux de retour d'expérience (REX) réalisés sur les événements indésirables relatifs à l'identification des usagers ;
- taux de formation/sensibilisation des professionnels de la structure à l'identitovigilance, par catégorie professionnelle*, etc.

Les établissements suivent les indicateurs pertinents au regard de leur activité et des directives éventuelles de niveau territorial ou régional. [RECO ES 02]

3 Gestion des risques

3.1 Principes généraux

3.1.1 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

³ [Plateforme QUAL HAS](#)

⁴ 3RIV, FIP 20 [Suivi d'indicateurs en identitovigilance](#)

à diminuer la probabilité de survenue des erreurs. Elle est classiquement distinguée en deux 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 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 d'établissement.

La GDR liée aux erreurs d'identification est la mission prioritaire des instances en charge de l'identitovigilance (cf. § 2.2), en association étroite avec les professionnels dédiés à la gestion des risques de la structure : direction ou service qualité gestion des risques, coordonnateur de la gestion des risques associés aux soins, responsable du système de management de la qualité de la prise en charge médicamenteuse⁵, référent local en identitovigilance, référents des différentes vigilances réglementaires (notamment pour l'hémovigilance, la matériovigilance, la pharmacovigilance, la réactovigilance), responsable de la sécurité des systèmes d'information, correspondants des structures sous-traitantes (biologie, EFS, CTSA, etc.).

3.1.3 Elaborer 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, etc.) ;
- par criticité (produit de la fréquence prévisible et du score de gravité potentielle des conséquences sur la sécurité de l'utilisateur).

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 professions concernées 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.

⁵ Voir l'arrêté du 6 avril 2011 relatif au management de la qualité de la prise en charge médicamenteuse et aux médicaments dans les établissements de santé

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 services ou structures :**
 - assurant l'accueil non programmé de patients (urgences, maternité, santé mentale, etc.) en raison du grand nombre de passages et de l'accueil d'usagers non connus,
 - réalisant l'accueil de façon délocalisée avec des applications autres que le référentiel d'identités,
 - réalisant des actes à risques (bloc opératoire, radiothérapie, etc.),
 - faisant assurer l'accueil par des professionnels non aguerris,
 - accueillant des usagers non communicants,
 - dont le turn-over des professionnels est élevé.
- **certains usagers :**
 - incapables de décliner leur identité (dément, confus, non francophone, inconscient, etc.),
 - utilisant des identités non vérifiables (exemple : détenu dont l'identité est enregistrée par les services de la justice, source de fausse identité délivrée par le détenu et/ou d'erreurs d'écriture par le greffe),
 - susceptibles, faute de couverture sociale, d'utiliser frauduleusement l'identité d'un autre (cf. § 3.2.6),
 - utilisant des traits différents dans la vie courante,
 - partageant un nom et un prénom commun à de nombreux autres usagers ;
- **certaines pratiques réalisées dans des conditions non sécuritaires du fait :**
 - d'interruptions de tâches,
 - de partage d'actions (réalisation de prélèvements par 2 personnes, remplacement, etc.),
 - etc.

3.1.3.3 Exemples de risques a priori dans un établissement de santé

<i>Types d'erreurs</i>	<i>Par qui, où, quand ?</i>	<i>Conséquences possibles</i>
Erreur de saisie des traits d'identité	Professionnels administratifs assurant l'accueil des usagers (service des entrées, consultations) Personnels soignants (urgences, maternité, admission directe dans un service, etc.)	Création inappropriée d'un nouveau dossier (doublon) ou, au contraire utilisation d'un mauvais dossier (collision)
Défaut de recherche d'un enregistrement préexistant ou erreur de sélection d'un dossier à l'admission		Perte de synchronisation avec des données préexistantes, erreur de facturation
Validation inappropriée d'une identité		Niveau de confiance non adapté, transmission non autorisée du matricule INS
Utilisation frauduleuse de l'identité d'un autre usager	Usager	Collision avec implications multiples sur la sécurité des soins, des données, la facturation Décision erronée du professionnel sur la base de mauvaises informations
Choix d'un mauvais dossier pour enregistrer des soins	Tous professionnels des services de soins, médico-techniques, brancardiers	Mauvaise attribution des données (collision)
Défaut de vérification « au lit du patient »		Erreur de personne pour la réalisation d'un acte technique
Interprétation incorrecte de l'identité		
Erreur de dossier, de patient, d'étiquetage lors d'un acte de soins, une demande d'examen, un prélèvement, etc.	Services de soins, bloc opératoire	Réalisation de l'acte sur le mauvais patient ou du mauvais côté Défaut de réalisation de l'examen Mauvaise attribution des résultats Erreur de diagnostic Retard de prise en charge

3.1.3.4 Exemples de barrières de sécurité

<i>Typologie des risques de dysfonctionnements</i>	<i>Actions préventives</i>
Saisie des traits d'identité lors de l'accueil de l'usager	Procédure d'accueil administratif, formation des agents, organisation du contrôle de cohérence a <i>posteriori</i> , etc.
Sélection du dossier dans lequel vont être enregistrées des informations de santé	Procédure d'identitovigilance en service de soins, sensibilisation en staffs de service, outils de communication, etc.
Réalisation de gestes techniques chez un patient	
Remise ou envoi de documents de coordination des soins	Procédure de sortie des usagers, formation des professionnels concernés, etc.
Utilisation d'une fausse identité par l'usager	Procédure permettant de dépister les usurpations et d'anticiper les mesures à prendre lors d'une suspicion de substitution d'identité
Défaut de connaissance des procédures	Audit des connaissances et des pratiques, formation initiale et continue, etc.

3.1.4 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.

3.1.4.2 Organisation

3.1.4.2.1 Signalement des EI

Les anomalies en rapport avec l'identification primaire ou secondaire – potentielles ou 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, etc.) ;
- d'identifier s'il s'agit d'EI liés à l'identification primaire ou à l'identification secondaire de l'utilisateur ;
- 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 permette la catégorisation des EI avec des attributs multiples – dont « erreur d'identitovigilance » – afin de pouvoir identifier ceux qui sont liés à des erreurs d'identification et de produire des statistiques pertinentes qui seront mises à disposition des instances stratégiques et opérationnelles en charge de l'identitovigilance.

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 indésirables⁶, au titre des obligations réglementaires en vigueur relatives aux vigilances et aux événements indésirables graves associés à des soins (EIGS)⁷ ;
- d'une alerte des parties prenantes lorsque l'événement a permis la propagation d'une identité erronée.

Il est également de bonne pratique de partager (en interne à la structure voire en externe, au niveau territorial et/ou régional⁸) les informations relatives à des erreurs inhabituelles d'identification primaire ou secondaire 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 retours d'expériences (REX) qui comprennent systématiquement :

- une analyse des facteurs institutionnels, organisationnels et humains ayant conduit à l'erreur ;

⁶ [Portail de signalement des événements indésirables](#)

⁷ Article R. 1413-68 du code de la santé publique

⁸ Par exemple comité consultatif régional en identitovigilance, structure régionale d'appui à la qualité des soins et à la sécurité des patients mentionnée à l'article R. 1413-75 du CSP, etc.

- la mise en œuvre d’actions correctives et/ou préventives 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, etc.

Les REX doivent être réalisés selon une méthode validée par la HAS^{9 10} :

- 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 », accompagnée par la CIV, 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 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 apporté par la structure régionale d’appui (SRA) à la qualité des soins et à la sécurité des patients¹¹.

Les REX font systématiquement l’objet de comptes rendus anonymisés qui sont transmis à l’instance opérationnelle de la structure.

3.1.4.3 Exemples d’événements indésirables

Événements indésirables	Conséquences
Administration d’un traitement au mauvais patient	Effets non attendus chez le patient ayant reçu le traitement, absence de traitement chez l’autre patient
Rangement d’un compte-rendu (d’examen, de consultation, d’hospitalisation) dans un mauvais dossier de soins	Attribution d’antécédents incorrects au patient, erreurs sur le traitement à mettre en place, retard diagnostique, etc.
Erreur de validation d’une identité	Envoi inapproprié de données avec un matricule INS
Prescriptions réalisées dans le mauvais dossier	Traitements inappropriés, iatrogénie
Absence d’étiquette ou erreur d’identification d’un prélèvement au bloc opératoire	Erreur ou retard diagnostique conduisant à un traitement inapproprié (ou à l’absence de prise en charge) Nécessité de réintervenir pour refaire le prélèvement
Identification incomplète sur une demande de produits sanguins labiles	Retard de délivrance par la structure de délivrance (EFS, CTSA, dépôt de produits sanguins labile)
Utilisation frauduleuse de la carte vitale d’un usager déjà connu	Collisions entre les données de santé de 2 usagers

⁹ Cf. la [synthèse de la Prévention Médicale](#)

¹⁰ [L’analyse des événements indésirables associés aux soins eias mode d’emploi guide méthodologique – Guide HAS FORAP : l’analyse des événements indésirables associés aux soins \(EIAS\)](#)

¹¹ L’ARS peut également décider de l’intervention de la SRA, si elle l’estime nécessaire, c’est-à-dire même en l’absence de demande du signalant (articles 1413-74 du CSP et suivants).

3.1.4.4 Exemples de barrières de sécurité

Typologie des dysfonctionnements	Actions correctives
Erreur d'identification primaire	Réaliser une évaluation des pratiques professionnelles, faire évoluer la procédure d'accueil administratif, sensibiliser les agents, mettre en place ou renforcer les contrôles de cohérence <i>a posteriori</i> , etc.
Erreur d'identification secondaire	Réaliser une évaluation des pratiques professionnelles, faire évoluer la procédure d'identitovigilance en service de soins, proposer des actions de type <i>patient traceur</i> , etc.
Remise ou envoi de documents de coordination des soins	Réaliser un audit des pratiques, réviser ou formaliser la procédure de sortie des patients, former et sensibiliser les professionnels concernés, etc.

3.2 Sécurisation des démarches d'identification primaire

3.2.1 Règles générales à appliquer

L'identification primaire comprend l'ensemble des opérations destinées à attribuer une identité à un usager physique qu'il s'agisse d'une première prise de contact avec l'utilisateur 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. RNIV 1 § 3).

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 assurant l'accueil des usagers après les actions de formation et de sensibilisation de tous les professionnels ;
- 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 ;
- la sécurisation de la création des identités par une organisation adaptée (par exemple : organisation d'un contrôle différé de cohérence de l'identité par un professionnel différent de celui qui a effectué la saisie ; mise en place d'applications informatiques aidant la détection d'erreurs courantes, etc.) ;
- la déclaration systématique des anomalies détectées secondairement par le système de signalement des événements indésirables (cf. § 3.1.4.2.1) ou par un logiciel dédié à l'identitovigilance, etc.

Il est rappelé, en outre, qu'il est interdit de pratiquer des « validations automatiques » des identités au bout d'un certain délai, sans passer par l'étape obligatoire de contrôle de cohérence des traits de l'identité avec ceux portés sur un dispositif d'identification à haut niveau de confiance (cf. RNIV 1 [EXI PP 09]).

3.2.2 Sécuriser l'utilisation des identités

3.2.2.1 Maitrise de la gestion des identités¹²

L'utilisation d'un référentiel d'identités (RI) unique au sein d'un même domaine d'identification permet de garantir la cohérence des données d'identité dans l'ensemble des logiciels métiers partageant les données personnelles des usagers pris en charge, et œuvre ainsi en faveur d'une sécurisation de l'identité.

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 13]

Cette garantie n'est cependant réellement obtenue que si la gestion des identités (création, modification, attribution d'un niveau de confiance, appel au téléservice INSi, etc.) est réalisée uniquement dans le RI.

Dans certaines structures, la création d'identités est réalisée dans différentes applications (urgences, consultations, dossier patient informatisé, gestion administrative des patients).

Il est recommandé que l'entière gestion (création, modification, appel au téléservice INSi, attribution d'un statut ou d'un attribut) de l'identité soit réalisée au sein d'un référentiel unique d'identités. [RECO ES 08]

Dans ce scénario qui doit être la cible, le logiciel doit bloquer tout flux de création / modification d'identités en provenance d'un autre logiciel.

Lorsque l'atteinte du scénario cible n'est pas possible (à court ou moyen terme), il reste **toléré de permettre la création d'une identité, au statut *Identité provisoire***, dans un logiciel autre que le logiciel « RI unique ». Les autres actions (validation de l'identité, modification, qualification, etc.) ne doivent pas être possibles dans ces autres logiciels.

Une identité créée dans un autre outil que le référentiel unique d'identités ne peut être intégrée qu'au statut identité provisoire. Les actions de modification, validation, qualification de l'identité ne peuvent être réalisées que dans le référentiel unique d'identités. [EXI SI 36]

Dans l'outil métier, il est possible de modifier certains traits complémentaires (hors nom et prénom utilisé).

A noter : l'appel au téléservice INSi pour réaliser une opération de vérification de l'INS est possible à partir de tout logiciel et n'est pas réservé au logiciel RI, contrairement à l'opération de récupération de l'INS. En effet, tout logiciel qui intègre des données de santé référencées avec l'INS en provenance d'un autre domaine d'identification est censé pouvoir effectuer une vérification de cette INS à réception de ces données.

3.2.2.2 Prévention et gestion des collisions

Une collision correspond à l'utilisation d'une même identité 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.

¹² 3RIV MEM 05 : [Dans quel dossier gérer les identités numériques ?](#)

Elle fait courir le risque de prendre des décisions de prise en charge au regard des données de santé d'une autre personne, ce qui 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 notamment 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 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 font 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 identités

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 12]

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 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. § 2.5.4.2). Un dispositif d'alerte spécifique aux structures concernées doit alors être mis en œuvre.

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 concernés¹³ doit, en priorité, imputer 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, etc.

Elle doit faire l'objet d'une information écrite (courrier postal, messagerie sécurisée) aux correspondants en précisant les modifications apportées.

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 ;

¹³ [Article 19 du Règlement général de protection des données \(RGPD\)](#)

- 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

Chaque structure doit régulièrement contrôler la qualité de son référentiel d'identités, notamment à la recherche de doublons, d'identités incohérentes ou de signaux d'alerte, par exemple, âge >120 ans, sexe incohérent avec le genre habituellement associé au prénom, etc. Elle doit aussi s'interroger sur la qualité des identités précédemment validées dont la fiabilité dépend du processus de validation utilisé (notamment par la pratique contestable et maintenant interdite de « validation automatique » au-delà d'un certain délai).

La mise en application des exigences relatives à l'emploi de l'Identité Nationale de Santé doit faire l'objet d'un audit préalable de la base d'identités¹⁴. À cette occasion, il est nécessaire que les identités non associées à un document d'identité à haut niveau de confiance (ou une trace de la pièce présentée) soient rétrogradées au statut *Identité provisoire* jusqu'à ce qu'un contrôle de cohérence des traits soit réalisé à l'occasion d'une nouvelle venue de l'utilisateur. [EXI ES 03]

3.2.2.5 Fusion d'identités au sein du domaine d'identification

La fusion des identités ne peut être réalisée que par des professionnels spécialement formés et habilités. [RECO ES 03].

Elle est décrite dans une procédure spécifique (cf. § 2.5.3). Lorsque les dossiers à fusionner comportent des données médicales, la cohérence entre les dossiers concernés doit être de préférence validée par un médecin afin d'éviter tout risque de collision. Chaque établissement détermine et formalise sa politique de fusion de dossiers, en particulier en termes d'identité à conserver (exemples : celle dont l'identité a le plus haut niveau de confiance ou la plus riche en termes d'information médicale, etc.).

Tout logiciel référentiel d'identités doit permettre de réaliser une fusion d'identité. Une fois la fusion réalisée, l'ensemble des documents doit être rassemblé sous l'identité maître (cf. RNIV 1 [EXI SI 34]).

La fusion d'identités ne peut être réalisée que dans le référentiel unique d'identités. [EXI SI 37]

Si, lors de la fusion entre 2 identités de statuts différents, l'identité maître ne comporte plus le matricule INS, il sera nécessaire de réitérer l'opération de récupération par appel au téléservice INSi et d'attribuer un nouveau statut de confiance, selon la procédure en vigueur.

Le système d'information doit garder une trace des actions effectuées (cf. RNIV 1 [EXI SI 14])

Lorsque la fusion a été réalisée, il faut s'assurer que l'information est transmise aux acteurs concernés, internes et externes à la structure, et que l'ensemble des pièces du dossier est associé à la bonne identité. Il peut être nécessaire de répercuter la fusion réalisée dans les logiciels non directement interfacés avec le référentiel d'identités. Celle-ci doit faire l'objet d'une procédure spécifique et confiée aux référents des logiciels métiers concernés (cf. § 2.5.4.3.4).

3.2.3 Sécuriser l'enregistrement de l'identité locale

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

¹⁴ Référentiel INS

sein de chaque structure à exercice collectif. [EXI PP 13]

3.2.3.1 Modification d'identité

La modification d'une identité n'est autorisée que pour des personnels habilités de la structure qui doivent être en nombre limité. Les modifications de traits stricts d'identités et des noms et prénoms utilisés ne peuvent être réalisées que dans le référentiel unique d'identité (cf. [EXI SI 36]). Elle est décrite dans une procédure interne spécifique (cf. § 2.5.3).

Elle est à réaliser conformément à la procédure relative au recueil de l'identité. Le système d'information doit garder une trace des modifications effectuées (cf. RNIV 1 [EXI SI 14]).

Lorsque la modification a été enregistrée, il faut s'assurer que l'information est transmise à tous les acteurs concernés.

Remarque : le rattachement à une nouvelle 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 d'une identité, il est recommandé de mettre en place des mécanismes de contrôle de la qualité de la saisie. Après avoir vérifié les données enregistrées par comparaison à une pièce d'identité officielle, on peut ajouter d'autres éléments de vérification, par exemple :

- demander à l'utilisateur (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'utilisateur les traits imprimés ou visualisés à l'écran ;
- faire contrôler *a posteriori* la cohérence des données de l'identité par une autre personne avec les traits portés par le document d'identité enregistré¹⁵.

Le tableau ci-dessous illustre quel niveau de sécurité associer à ces pratiques, à prendre en compte lors de la formalisation de la procédure d'identification primaire par la structure.

Mécanisme de contrôle 1	Mécanisme de contrôle 2	Niveau de sécurité
Comparaison de la cohérence des traits saisis avec ceux présents sur une pièce d'identité	Aucun	Faible
	Déclinaison orale de son identité par l'utilisateur	Faible
	Relecture par l'utilisateur des informations enregistrées, à l'écran ou sur un document imprimé	Moyen
	Contrôle <i>a posteriori</i> de la saisie par un professionnel différent de celui ayant réalisé la saisie initiale en s'appuyant sur le document d'identité enregistré	Fort

3.2.4 Sécuriser l'utilisation de l'INS

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

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

¹⁵ Sous réserve du respect des règles de conservation des données en vigueur

- de sélection d'un mauvais bénéficiaire lors de l'interrogation du téléservice par utilisation de la carte Vitale ;
- d'un mauvais contrôle de cohérence à la réception des données renvoyées par le téléservice (cf. RNIV 1 § 4.5).

Lors du constat de l'erreur d'attribution d'une INS, la structure doit informer l'ensemble des professionnels avec lesquels elle a partagé des données.

3.2.4.2 Constat d'un écart sur l'INS a posteriori

Le statut *Identité qualifiée* 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 (cf. § 3.2.6), d'une erreur lors du contrôle de cohérence réalisé au moment de la qualification (cf. RNIV 1 § 4.5), 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. RNIV 1 § 3.2.2). La structure apprécie la pertinence de réaliser une déclaration d'évènement indésirable (s'il s'agit d'une collision de données en particulier).

3.2.5 Sécuriser la gestion des identités approchantes

3.2.5.1 Généralités

Il est important de définir comment identifier et gérer les identités 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 (risque de collision) ;
- lors de la prise en charge (risque de collision par erreur de dossier, d'étiquette, etc.) ;
- 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 *recupérées* 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 approchantes dans les opérations administratives et soignantes. Il est conseillé de formaliser une procédure qui décrit :

- comment faire la liste des identités concernées (outils de recherche de doublons, calcul de ressemblance, lorsqu'ils sont proposés par le système d'information, signalement interne, etc.) ;
- dans quelles conditions utiliser l'attribut *Identité homonyme* – qui n'est pas réservé aux seuls homonymes vrais (cf. RNIV 1 § 3.2.3) – 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, etc.

3.2.5.2 Information des parties prenantes

Lors de l'arrivée d'un usager dont l'identité est très proche d'un ou de plusieurs usagers enregistrés dans la base de données locale, il est important de prévoir la modalité de diffusion de l'alerte aux différents correspondants (laboratoire, service d'imagerie, EFS, CTSA, etc.) pour limiter également le risque d'erreur à leur niveau : contact téléphonique, alerte par message, étiquetage spécifique, etc.

3.2.5.3 Autres situations imposant la gestion d'identités approchantes

Lors de l'accueil d'un usager qui correspond à une identité préexistante, sans qu'il soit possible de certifier qu'il s'agit bien de la même personne, il est recommandé de l'enregistrer sous une nouvelle identité en attendant de pouvoir statuer sur la possibilité de fusionner ultérieurement ces identités. [RECO ES 04]

C'est le cas, par exemple dans les cas :

- de suspicion de substitution frauduleuse d'identité (cf. § 3.2.6) par un usager ;
- de réception de données d'identité dont la qualité n'est pas jugée suffisante par le prestataire (cf. RNIV 1 § 4.10.4).

Mieux vaut en effet ne pas risquer de créer une collision entre des identités de qualité incertaine et ainsi garantir la sécurité des soins. Le traitement de ces doublons potentiels – ou de certains d'entre eux – pourra être réalisé *a posteriori*.

Remarque : la création de doublon fait courir d'autres risques, comme celui de ne pas pouvoir avoir accès aux informations de santé et résultats d'examens antérieurs.

3.2.6 Gérer une suspicion d'utilisation frauduleuse d'identité

Il n'est pas rare que des usagers sans couverture sociale se servent de l'identité d'usagers enregistrés auprès de l'assurance maladie, avec ou sans leur accord, afin de bénéficier de leurs droits. Cette substitution frauduleuse, qui relève de la qualification pénale d'escroquerie¹⁶, est potentiellement dangereuse pour la santé lorsqu'elle entraîne la collision de données entre le fraudeur et un usager déjà enregistré dans la structure. Elle ne permet plus aux professionnels de santé d'accéder à des informations fiables en termes d'antécédents, d'allergies, d'examens complémentaires et peut être responsable de diagnostics ou traitements erronés.

En règle générale, ces tentatives de fraudes sont plus fréquentes lors du recours à des soins non programmés (urgences) où seul un document de couverture sociale est présenté.

¹⁶ Articles 313-1 et 313-2 du code pénal

Il est important que les structures exposées à ce risque définissent :

- les messages de prévention, de dissuasion et d'information des usagers ;
- les signaux d'alerte qui permettent de suspecter la fraude (exemples : discordances entre l'utilisateur présent et les informations du document présenté (âge, sexe, adresse, etc.) et/ou préalablement enregistrées dans le système d'information (données administratives voire médicales) ; réponses évasives ou contradictoires lors de la vérification de l'identité, etc.) ;

Remarque : la comparaison de la photographie présente sur les documents fournis avec l'aspect physique de l'utilisateur est souvent peu contributive, les photographies pouvant être anciennes et peu ressemblantes.

La conduite à tenir lors d'une suspicion de fraude comprend des mesures de sécurisation telles que :

- la création d'un dossier provisoire, en utilisant l'attribut *identité douteuse*, pour ne pas risquer de collision avec un dossier précédent ;
- le signalement interne de l'événement indésirable (cf. § 3.1.4.2.1) ;
- l'identification des documents transmis qui n'appartiennent pas à l'utilisateur ;
- 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'utilisateur dont l'identité a été empruntée, etc.).

Il est recommandé de réaliser un signalement externe aux autorités compétentes en cas de suspicion d'utilisation frauduleuse de l'identité d'autrui pour obtenir indument des prestations sanitaires. [RECO ES 05]

3.3 Sécurisation des démarches d'identification secondaire

3.3.1 Règles générales à appliquer

L'identification secondaire consiste à s'assurer systématiquement de la cohérence entre l'identité de l'utilisateur physique et l'identité portée sur la prescription / le document / le dossier / le geste technique qui le concerne(nt). Plusieurs recommandations peuvent être faites pour améliorer les pratiques dans ce domaine. Il s'agit de vérifier que l'utilisateur 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'utilisateur sans risque d'erreur (durée de séjour, fréquence de prise en charge itérative, HAD) ;
- de la possibilité de faire participer l'utilisateur à sa sécurité (adhésion, compréhension, etc.) ;
- des dispositifs d'identification pouvant être utilisés dans la structure.

3.3.2 Sécuriser l'identification de l'utilisateur

3.3.2.1 Identification orale

Dans les échanges quotidiens soignant-soigné, il est possible d'employer le nom et prénom utilisé.

Néanmoins, dans le cadre de la réalisation d'un soin, il est demandé à l'utilisateur de décliner son identité par le biais de questions ouvertes, à **minima, nom de naissance, premier prénom de naissance, date de naissance**.

Les usagers doivent être sensibilisés à cette pratique et être encouragés à y participer.

L'identité pourra être plus ou moins détaillée selon les circonstances de prise en charge et le type d'acte réalisé.

3.3.2.2 Dispositifs d'identification physique

Plusieurs dispositifs peuvent participer à l'identification de l'utilisateur, tels que la pose d'un bracelet, l'utilisation d'une photographie dans son dossier¹⁷. L'usage veut que le dispositif d'identification soit proposé systématiquement à tous les patients, en respectant leur droit de refus¹⁸, afin de ne pas stigmatiser une population et maintenir le lien soignant-soigné.

Il est recommandé d'utiliser un dispositif d'identification physique pour tous les usagers incapables de décliner leur identité. [RECO ES 06]

Il est également particulièrement utile pour les usagers :

- admis pour une hospitalisation (y compris en hospitalisation de jour) ;
- bénéficiant d'un acte de soins pour lequel une erreur d'identité peut être particulièrement critique (chirurgie, endoscopie, imagerie interventionnelle, transfusion, radiothérapie, chimiothérapie, traitement allergisant, etc.) ;
- nouveaux nés ;
- avec lesquels la communication est difficile : non francophone, patient confus, inconscient, dément, etc.
- décédés, non porteurs d'un bracelet au cours de leur séjour, en vue de leur transfert en chambre mortuaire, etc.

Leur utilisation doit faire l'objet d'une procédure qui décrit :

- l'information de l'utilisateur, 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 de traçabilité dans le dossier de l'utilisateur ;
- 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, etc.

Il faut éviter la transcription manuelle de l'identité de l'utilisateur sur le bracelet (source d'erreurs) et privilégier les bracelets comportant une identité imprimée à partir des données informatisées (cf. RNIV 1 § 4.9.2).

3.3.3 Sécuriser l'utilisation des documents de prise en charge

3.3.3.1 Identification des informations relatives à l'utilisateur

Les structures de santé doivent veiller à ce que tous les documents liés à la prise en charge d'un usager (courrier, feuille de surveillance, demande d'examen, document de transfert, etc.) soient identifiés

¹⁷ Sous réserve du respect du droit à l'image et de la réglementation applicable

¹⁸ Hors situations obligatoires : bloc opératoire, décès, etc.

correctement (cf. RNIV 1 [EXI SI 16], [EXI PP 21] et [EXI PP 22]). Il est important de vérifier qu'aucune équivoque n'est possible sur la nature des traits, notamment dans les échanges entre structures différentes (cf. RNIV 1 [EXI SI 11]).

Pour un document adressé par une source externe qui utiliserait d'autres modalités d'identification, une procédure doit en préciser les modalités de gestion pour limiter le risque d'erreur d'attribution. Par exemple, il peut être recommandé, en cas de discordances avérées :

- de coller l'étiquette de l'utilisateur sur chaque page du document papier reçu, en veillant à ce que celle-ci ne recouvre pas les données d'identité présentes sur l'original ;
- d'utiliser une procédure spécifique pour identifier les documents externes numérisés avant de les joindre dans le dossier informatique de l'utilisateur ;
- de signaler à l'expéditeur l'anomalie constatée en termes d'identification de l'utilisateur afin qu'il puisse la corriger à son niveau.

3.3.3.2 Cohérence entre documents

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

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

Remarque : les couples mariés doivent faire l'objet d'une attention particulière en cas de séjour simultané dans la même structure, et en particulier s'ils sont hospitalisés dans la même chambre. Il en est de même pour les personnes ayant des identités approchantes (cf. § 3.2.5) ainsi que lors de la prise en charge de jumeaux.

3.4 Formation et sensibilisation à l'identitovigilance

3.4.1 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 conséquences.

3.4.2 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 doivent faire partie des actions du plan de formation annuel des établissements de santé. [EXI ES 04]

Elles concernent l'ensemble des professionnels intervenant dans la structure et doivent prendre en compte tous les aspects de la documentation qualité dédiée (cf. RNIV 1 § 5). Des formations dédiées peuvent être organisées en fonction des objectifs attendus et de la population concernée. Elles peuvent concerner les correspondants externes : ambulanciers, professionnels et structures adressant des usagers, plateaux techniques, etc.

Les structures qui le souhaitent peuvent mettre en œuvre des processus d'habilitation des professionnels, conditions préalables à l'obtention de droits d'accès et de modifications :

- formation initiale avec évaluation de l'appropriation des concepts ;
- formation continue, notamment pour les professionnels absents au-delà d'un certain délai ;
- évaluation annuelle, notamment pour les professionnels en charge de l'identification primaire dans les lieux d'accueil de la structure.

Des évaluations régulières, par contrôle de connaissance ou audit de pratique, sont recommandées 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, etc.

3.4.2.2 Information et sensibilisation des usagers

Les usagers et leur famille doivent être informés au plus tôt des documents qui leur seront demandés tout au long de leur prise en charge programmée (document d'identité officiel notamment).

Une attention toute particulière doit être portée à la communication réalisée auprès des usagers (site Web, affichage, livret ou borne d'accueil, explications orales, etc.), 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'utilisateur ne peut s'opposer à l'utilisation de son INS mais doit en être informé¹⁹. Cette information doit être partagée dans les instances où siègent des représentants d'usagers, dont la *Commission des usagers* (CDU).

Il est fortement recommandé d'informer l'utilisateur de l'impossibilité de qualifier son INS, et de ses conséquences en raison de discordances entre les traits d'identités de l'INS et du dispositif d'identification de haut niveau de confiance, afin qu'il puisse réaliser les démarches nécessaires pour corriger le problème (cf. RNIV1 § 4.7).

¹⁹ Cf. Référentiel INS

ANNEXE I - Exigences et recommandations applicables

Exigences et recommandations spécifiques aux établissements de santé

N°	Libellé de l'exigence	Evolution/V1.3
EXI ES 01	Des instances stratégique et opérationnelle dédiées à l'identitovigilance doivent être mises en place par les établissements de santé et les groupements de structures.	
EXI ES 02	Un référent en identitovigilance doit être identifié dans tout établissement de santé.	
EXI ES 03	La mise en application des exigences relatives à l'emploi de l'identité nationale de santé doit faire l'objet d'un audit préalable de la base d'identités. À cette occasion, il est nécessaire que les identités non associées à un document d'identité à haut niveau de confiance (ou une trace de la pièce présentée) soient rétrogradées au statut <i>Identité provisoire</i> jusqu'à ce qu'un contrôle soit réalisé à l'occasion d'une nouvelle venue de l'utilisateur.	
EXI ES 04	La formation et la sensibilisation des professionnels à l'identitovigilance doivent faire partie des actions du plan de formation annuel des établissements de santé.	
EXI ES 05	Les structures communiquent le nom et les coordonnées du référent en identitovigilance à l'instance régionale (référent régional en identitovigilance, cellule régionale d'identitovigilance, etc.)	Ajout
RECO ES 01	Il est nécessaire de mettre en place des précautions particulières lorsqu'un professionnel accède à des données d'un patient qu'il ne prend pas directement en charge, notamment dans le cadre de l'urgence (procédure « bris de glace ») et de l'accès des services de veille sanitaire des ARS à des données devant donner lieu à un signalement de maladie à déclaration obligatoire (MDO).	
RECO ES 02	Les établissements suivent les indicateurs pertinents au regard de leur activité et des directives éventuelles de niveau territorial ou régional.	
RECO ES 03	La fusion des identités ne peut être réalisée que par des professionnels spécialement formés et habilités.	
RECO ES 04	Lors de l'accueil d'un usager qui correspond à une identité préexistante, sans qu'il soit possible de certifier qu'il s'agit bien de la même personne, il est recommandé de l'enregistrer sous une nouvelle identité en attendant de pouvoir statuer sur la possibilité de fusionner ultérieurement ces identités.	
RECO ES 05	Il est recommandé de réaliser un signalement externe aux autorités compétentes en cas de suspicion d'utilisation frauduleuse de l'identité d'autrui pour obtenir indument des prestations sanitaires.	
RECO ES 06	Il est recommandé d'utiliser un dispositif d'identification physique pour tous les usagers incapables de décliner leur identité.	

RECO ES 07	L'établissement de santé formalise une politique d'identitovigilance en accord avec la politique qualité et sécurité conduite par la structure ou par le groupe auquel elle appartient.	Ajout
RECO ES 08	Il est recommandé que l'entière gestion (création, modification, appel au téléservice INSi, attribution d'un statut ou d'un attribut) de l'identité soit réalisée au sein d'un référentiel unique d'identités	Ajout

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

N°	Libellé de l'exigence	Evolution /Version 1.3
EXI SI 01	<p>Le système d'information doit permettre d'effectuer la recherche d'une identité à partir :</p> <ul style="list-style-type: none"> de la saisie de la date de naissance, éventuellement complétée par les premiers caractères du nom ou du prénom. du matricule INS 	Précision apportée
EXI SI 02	<p>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 13 caractères du NIR avec leur validation par la clé de contrôle est obligatoire pour toute recherche à partir du matricule INS.</p>	Précision apportée
EXI SI 03	<p>Lors de la recherche d'un usager dans la base d'identités locale, 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 <i>Nom de naissance</i> et <i>Nom utilisé</i>, <i>Premier prénom de naissance</i> et <i>Prénom utilisé</i>. L'utilisation d'une barre de recherche multicritères est interdite. Il est obligatoire de disposer de champs d'interrogation distincts : date de naissance, nom, prénom.</p>	Précision apportée
EXI SI 04	<p>Les traits d'identification doivent faire l'objet de champs spécifiques dans le système d'information.</p>	
EXI SI 05	<p>Le système d'information doit permettre la saisie des traits complémentaires <i>Nom utilisé</i> et <i>Prénom utilisé</i>.</p>	
EXI SI 06	<p>Les informations récupérées du téléservice INSi font l'objet d'un stockage et d'une traçabilité au niveau du système d'information de santé.</p>	
EXI SI 07	<p>Tout système d'information en santé doit permettre d'attribuer un des 4 statuts de confiance à chaque identité numérique stockée.</p>	
EXI SI 08	<p>Le système d'information doit garantir que seul le statut <i>Identité qualifiée</i> permette le référencement des données de santé échangées avec le matricule INS, en conformité avec la réglementation applicable.</p>	
EXI SI 09	<p>Pour les identités comportant un attribut <i>Identité douteuse</i> ou <i>Identité fictive</i> il doit être informatiquement rendu impossible :</p> <ul style="list-style-type: none"> d'attribuer un statut autre que celui d'<i>Identité provisoire</i> ; de faire appel au téléservice INSi. 	
EXI SI 10	<p>Le type de dispositif d'identification ayant servi au recueil de l'identité doit être enregistré. Seul un document à haut niveau de confiance, ou son équivalent, doit autoriser l'attribution des statuts <i>Identité validée</i> ou <i>Identité qualifiée</i>.</p>	
EXI SI 11	<p>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 concernés.</p>	

EXI SI 12	Après attribution du statut <i>Identité qualifiée</i> ou <i>Identité récupérée</i> , 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.	Transfert dans les RNIV2 et 3
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 permettre 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.	Suppression
EXI SI 16	L'affichage d'une identité doit comporter <i>a minima</i> le nom de naissance, le nom utilisé, le premier prénom de naissance, le prénom utilisé, la date de naissance, le sexe et le statut de l'identité.	Ajout
EXI SI 17	Sur chaque identité du résultat de la recherche, les chaînes de caractères correspondant à celles utilisées pour la recherche d'antériorité doivent être mises en évidence pour les champs nom de naissance, nom utilisé, premier prénom, prénom utilisé (mettre en gras, autre couleur, etc.).	Ajout
EXI SI 18	Le système d'information doit permettre la saisie du code 99999 si le lieu de naissance est inconnu.	Ajout
EXI SI 19	Le champ lieu de naissance ne doit pas être pré-rempli avec une valeur par défaut.	Ajout
EXI SI 20	Le système d'information doit gérer l'historique des codes communes et l'historique des codes pays, et ainsi proposer la commune ou le pays approprié(e) en fonction de la date de naissance de l'utilisateur.	Ajout
EXI SI 21	Le système d'information ne doit pas alimenter les champs <i>Nom utilisé</i> et <i>Prénom utilisé</i> par défaut. La copie à partir du champ nom de naissance ou premier prénom doit être une action volontaire de l'utilisateur, qui peut être facilitée par le système d'information.	Ajout
EXI SI 22	Le SI doit permettre l'emploi des attributs <i>homonyme</i> , <i>douteux</i> et <i>fictif</i> pour permettre aux professionnels de caractériser les identités nécessitant un traitement particulier.	Ajout (RECO SI 02 transformé en EXI)
EXI SI 23	En dehors de l'obtention de l'INS par l'Appli carte Vitale ou de la validation de l'identité par un dispositif d'identification électronique conforme eIDAS, la sélection par défaut du dispositif à haut niveau de confiance ou de son équivalent permettant de valider l'identité est interdite.	Ajout
EXI SI 24	Les systèmes d'information utilisés pour gérer les identités doivent permettre la gestion des copies numériques de pièce d'identité conformément aux règles décrites dans le présent référentiel.	Ajout
EXI SI 25	Le système d'information doit permettre, par paramétrage, d'autoriser ou interdire l'appel au téléservice INSi pour les identités au statut <i>Identité provisoire</i> .	Ajout
EXI SI 26	En première intention, le code officiel géographique du lieu de naissance ne doit pas être utilisé pour interroger le téléservice INSi par saisie des traits.	Ajout

EXI SI 27	Les traits utilisés pour l'interrogation du téléservice doivent être modifiables par l'utilisateur dans la fenêtre d'interrogation sans avoir à modifier l'identité locale.	Ajout
EXI SI 28	En cas de divergence portant sur l'un des 5 traits d'identité (nom de naissance, liste de prénoms, date de naissance, sexe, code officiel géographique du lieu de naissance) entre l'identité locale et l'INS retournée par le téléservice INSi, un écran de comparaison des traits doit être affiché et mettre en évidence les différences.	Ajout
EXI SI 29	Le premier prénom de naissance doit être cohérent avec le début de la liste des prénoms de naissance (tirets ou apostrophes ne doivent pas être considérés différents d'un espace).	Ajout
EXI SI 30	Le premier prénom de naissance doit rester modifiable par l'utilisateur quel que soit le statut de l'identité s'il reste cohérent avec le début de la liste des prénoms. Le statut de l'identité ne doit pas être impacté.	Ajout
EXI SI 31	Le système d'information doit accepter le Code Officiel Géographique (COG) retourné par le téléservice INSi y compris s'il est inconnu dans son référentiel interne.	Ajout
EXI SI 32	Dans un même domaine d'identification, il ne doit pas exister plusieurs identités numériques avec le même matricule INS (doublet d'INS). Un message d'alerte de l'utilisateur doit être proposé par le logiciel lors de la récupération d'une INS, si le matricule est déjà connu dans le domaine d'identification.	Ajout
EXI SI 33	En présence d'un contrat de confiance, le récepteur de l'identité doit faire appel à l'opération récupération du téléservice INSi pour une identité reçue au statut <i>identité qualifiée</i> , uniquement si celle-ci n'est pas déjà connue du SI local. Dans le cas où cette vérification est conforme, l'identité pourra être créée au statut <i>identité qualifiée</i> dans le SI local, sinon l'identité pourra être créée au statut <i>identité validée</i>	Ajout
EXI SI 34	En l'absence de contrat de confiance, l'identité reçue ne peut être créée qu'au statut <i>identité provisoire</i> si elle n'était pas préexistante dans le système d'information du receveur à un statut supérieur.	Ajout
EXI SI 35	Tout logiciel référentiel d'identités doit permettre de réaliser une fusion d'identités, quel que soit le statut des identités à fusionner. Une fois la fusion réalisée, l'ensemble des documents doit être rassemblé sous l'identité maître.	Ajout
EXI SI 36	Une identité créée dans un autre outil que le référentiel unique d'identités ne peut être intégrée qu'au statut identité provisoire. Les actions de modification, validation, qualification de l'identité ne peuvent être réalisées que dans le référentiel unique d'identités.	Ajout Spécifique RNIV 2 et 3
EXI SI 37	La fusion d'identités ne peut être réalisée que dans le référentiel unique d'identités.	Ajout Spécifique RNIV2 et 3
EXI SI 38	Le système d'information doit par paramétrage interne permettre à l'utilisateur de définir le statut de l'INS obtenue par l'Appli carte Vitale.	Ajout

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.	Transformée en EXI SI 22
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 relatives aux pratiques professionnelles (RNIV 1)

N°	Libellé de l'exigence	Evolution /Version 1.3
EXI PP 01	L'appel au téléservice INSi est obligatoire pour vérifier une INS reçue lorsque l'identité numérique n'existe pas ou qu'elle ne dispose pas d'un statut récupéré ou qualifié.	Remplacée par EXI SI 33
EXI PP 02	La création d'une identité requiert la saisie d'une information pour au moins 5 traits stricts : nom de naissance, premier prénom de naissance (simple ou composé), date de naissance, sexe et lieu de naissance.	Précisions apportées
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 et/ou utilisation de l'Appli carte Vitale, dans les cas d'usage où l'emploi du matricule INS est requis et autorisé.	Précisions apportées
EXI PP 04	Il est nécessaire de renseigner le maximum de traits complémentaires, selon les consignes que chaque structure définit, en restant dans la limite des données nécessaires à la prise en charge, dans le respect du principe de minimisation des données au sens RGPD.	Précisions apportées
EXI PP 05	Avant toute intégration de l'INS dans l'identité 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 ; cette méthode favorise et sécurise la récupération de l'INS correspondant à l'identité recherchée.	Précision apportée
EXI PP 07	L'attribution d'un niveau de confiance à toute identité est obligatoire.	
EXI PP 08	Afin d'utiliser une identité de confiance, il est indispensable de vérifier, au moins une fois, de préférence lors de la première prise en charge de l'usager, que le dispositif d'identification à haut niveau de confiance ou son équivalent, correspond à la personne concernée.	Reformulation
EXI PP 09	Seul un contrôle de cohérence de l'identité avec un dispositif à haut niveau de confiance ou un équivalent autorise sa validation. La nature de ce dispositif ou de son équivalent doit être enregistré dans le SI.	Reformulation
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.	Remplacée par l'EXI PP 21 et EXI PP 22

EXI PP 11	Dès lors que son identité est passée au statut <i>Identité qualifiée</i> , le matricule INS et les traits INS doivent être utilisés pour l'identification de l'utilisateur, 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.	Transfert dans les RNIV 2 et 3
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.	Transfert dans les RNIV 2 et 3
EXI PP 14	Les acteurs de santé impactés par la diffusion d'une erreur en lien avec l'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'utilisateur au sein d'une charte d'identitovigilance.	Transfert dans les RNIV 2 et 3
EXI PP 16	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.	Suppression de la mention « comme pour les autres traits stricts) »
EXI PP 17	L'enregistrement du <i>nom utilisé</i> est obligatoire lorsqu'il est différent du <i>nom de naissance</i> .	
EXI PP 18	L'enregistrement du <i>prénom utilisé</i> est obligatoire lorsqu'il est différent du <i>premier prénom de naissance</i> .	
EXI PP 19	Lorsque la date de naissance fournie par le document d'identité ou le dispositif d'identification est incomplète, il faut appliquer les consignes suivantes : <ul style="list-style-type: none"> • si seul le <i>jour</i> est inconnu, il est remplacé par le premier jour du mois (01/MM/AAAA) ; • si seul le <i>mois</i> n'est pas connu, il est remplacé par le premier mois de l'année (JJ/01/AAAA) ; • si le <i>jour ET le mois</i> ne sont pas connus, il faut saisir la date du 31 décembre de l'année de naissance²⁰(31/12/AAAA) ; • si l'<i>année</i> n'est pas connue précisément, on utilise l'année ou la décennie compatible avec l'âge annoncé ou estimé ; • si la <i>date de naissance</i> est inconnue, on enregistre 31/12 et une année ou décennie compatible avec l'âge annoncé ou estimé, par exemple, 31/12/1970. 	Ajout
EXI PP 20	Si l'INS proposée par le téléservice INSi est discordante de l'identité de l'utilisateur sur le nom de naissance, le premier prénom de naissance, le sexe ou la date de naissance, la récupération et la qualification de l'INS sont interdites. L'absence d'un trait d'identité de l'INS interdit la récupération	Ajout

²⁰ Cette consigne n'est pas applicable pour un enfant < 1 an hospitalisé (date d'entrée de prise en charge est antérieure à la date de naissance). Il est recommandé alors d'estimer approximativement le mois de naissance (01/mm/AAAA).

	et la qualification de l'INS. Les différences portant sur l'utilisation de tirets ou d'apostrophes ne doivent pas être considérées comme une discordance.	
EXI PP 21	<p>La première page d'un document de santé comporte obligatoirement les informations suivantes :</p> <ul style="list-style-type: none"> - Si l'identité de l'utilisateur est qualifiée : <ul style="list-style-type: none"> • nom de naissance, • premier prénom de naissance, • liste des prénoms, • date de naissance, • sexe, • lieu de naissance, • matricule INS suivi de sa nature (NIR ou NIA), • nom et prénom utilisé s'ils sont renseignés, • Datamatrix INS. <p>Dans le cas où le Datamatrix INS n'est pas pris en charge par le système d'information, il est possible de positionner cet élément sur une page distincte qui peut être positionnée à la fin du document de santé.</p> <ul style="list-style-type: none"> - Si l'identité de l'utilisateur n'est pas qualifiée : <ul style="list-style-type: none"> • nom de naissance, • premier prénom de naissance, • date de naissance, • sexe, • nom utilisé et prénom utilisé s'ils sont renseignés. <p>Les pages suivantes du document²¹ contiennent, <i>a minima</i> :</p> <ul style="list-style-type: none"> • nom de naissance, • premier prénom de naissance, • date de naissance, • sexe, • nom utilisé et prénom utilisé s'ils sont renseignés. 	Ajout
EXI PP 22	<p>Les étiquettes d'identification générées par le système d'information comportent <i>a minima</i>, les informations suivantes :</p> <ul style="list-style-type: none"> • nom de naissance, • premier prénom de naissance, • date de naissance, • sexe, • nom utilisé et prénom utilisé s'ils sont renseignés. 	Ajout
EXI PP 23	Le contrat de confiance ne peut être établi que si l'émetteur de la donnée s'engage à réaliser un contrôle de cohérence en utilisant un dispositif d'identification de haut niveau de confiance.	Ajout
RECO PP 01	Pour obtenir des résultats pertinents, il est fortement recommandé de limiter à 3 le nombre de caractères saisis pour effectuer la recherche d'un enregistrement à partir du nom ou du prénom.	Précision apportée
RECO PP 02	Il est important que toute difficulté rencontrée pour la récupération de l'INS ou la qualification de l'identité, du fait d'une incohérence non mineure, soient signalées comme événement indésirable et rapportées au niveau régional et national.	

²¹ Les traits d'identité, en page 2 et suivantes, peuvent être affichées en haut ou bas de page.

RECO PP 03	Afin de limiter les risques de collision, il n'est pas recommandé d'appeler le téléservice INSi pour des identités au statut <i>identité provisoire</i> s'il n'est pas possible de réaliser dans le même temps le contrôle de cohérence avec un dispositif d'identification de haut niveau de confiance ou son équivalent.	Ajout
RECO PP 04	En présence d'un contrat de confiance, le récepteur de l'identité peut faire appel à l'opération de récupération du téléservice INSi pour une identité reçue au statut <i>identité validée</i> afin d'attribuer le statut <i>identité qualifiée</i> dans le SI local si l'appel au téléservice INSi est fructueux. Si l'appel au téléservice INSi est infructueux, le statut de l'identité est <i>identité validée</i> .	Ajout

ANNEXE II – Glossaire des sigles utilisés

AAC :	Analyse approfondie des causes d'événements indésirables
ALARM(E) :	<i>Association of Litigation And Risk Management (Extended)</i> , technique d'AAC
ARS :	Agence régionale de santé
ATIH :	Agence Technique de l'Information sur l'Hospitalisation
CDU :	Commission des usagers
CIV :	Cellule d'identitovigilance
CI-SIS :	Cadre d'interopérabilité des systèmes d'information en santé
CME :	Commission ou Conférence Médicale d'Établissement
CPOM :	Contrat pluriannuel d'objectifs et de moyens
CREX :	Comité de retour d'expérience
CTSA :	Centre de transfusion sanguine des armées
DIM :	Département d'Information Médicale
DMP :	Dossier Médical Partagé
EI :	Événement indésirable
eIDAS :	<i>Electronic Identification, Authentication and Trust Services</i> (règlement européen pour accroître la confiance dans les transactions électroniques)
EIGS :	Événement indésirable grave associé à des soins
EPR :	Événement porteur de risques
ES :	Établissement de santé
ETP :	Équivalent temps plein
EXI :	Exigences rendues opposables par le RNIV
GDR :	Gestion des risques
GHT :	Groupement hospitalier de territoire
HAS :	Haute Autorité de santé
IHE PAM :	<i>Integrating the Healthcare Enterprise Patient Administration Management</i> (utilisation coordonnée de standards d'interopérabilité pour les échanges informatisés de données de santé)
INS :	Identité Nationale de Santé
INSEE :	Institut national de la statistique et des études économiques
INSi :	Téléservice de recherche et de vérification de l'identité nationale de santé (INS)
HAD :	Hospitalisation à domicile
IQSS :	Indicateurs qualité et sécurité des soins
oSIS :	Observatoire des systèmes d'information en santé
PP :	Pratiques professionnelles
QUALHAS :	Plateforme de recueil des IQSS gérée par la HAS
Reco :	Recommandation
REX :	Retour d'expérience
RGPD :	Règlement général de protection des données
RI :	Référentiel unique d'identités
RMM :	Revue de morbi-mortalité
RNIV 1 :	Référentiel national d'identitovigilance. Partie 1 (Points communs)

- RNIV 3 :** Référentiel national d'identitovigilance. Partie 3 (Identitovigilance en structure non hospitalière)
- SI :** Système d'information
- SIS :** Système d'information en santé
- SRA :** Structure régionale d'appui à la qualité des soins et à la sécurité des patients
- SSEI :** Système de signalement des événements indésirables
- SMR :** Soins médicaux et de réadaptation
- USLD :** Unité de soins longue durée

ANNEXE III Exemples d'organisation de gestion des identités

