IDENTITOVIGILANCE
NOUVELLE-AQUITAINE

Comité technique régional d'identitovigilance de Nouvelle-Aquitaine

REFERENTIEL DE BONNE PRATIQUE EN MATIERE D'IDENTITOVIGILANCE EN REGION NOUVELLE-AQUITAINE

Version 2 validée le 11 décembre 2018

Liste des contributeurs

- **A la mise à jour de la version 2**
  - Mme Tiphaine BONDY, assistante des vigilances, EFS Nouvelle-Aquitaine
  - Mme Céline DESCAMPS, cadre de santé, CHU de Bordeaux, CRIV
  - Mme Nadine DOUCEDE, infirmière référente métier, Hôpital privé Saint-Martin, Pessac
  - Mme Christelle NOZIERE, GIP ESEA, CRIV
  - Mme Dany OULEY, ingénieur qualité, Cellule d'identitovigilance et de rapprochement du CHU de Bordeaux
  - Dr Bernard TABUTEAU, pôle qualité et sécurité des soins, ARS Nouvelle-Aquitaine
  - Mme Françoise URSULET, CHU de Poitiers, CRIV.

- **A la version initiale**
  - Mme Marie-Pierre BAUDON, chargée de mission système d'information, ARS Nouvelle-Aquitaine
  - Dr Yann BLANCHARD, Département d'information médicale, Centre hospitalier de la Côte Basque
  - Mme Tiphaine BONDY, assistante des vigilances, EFS Nouvelle-Aquitaine
  - M. Patrick CHARPENTIER, représentant des usagers, Union nationale des associations agréées d'usagers du système de santé
  - Mme Myriem DEMIR, responsable du service des admissions, CHU de Bordeaux
  - Mme Céline DESCAMPS, cadre de santé, CHU de Bordeaux
  - Mme Nadine DOUCEDE, infirmière référente métier, Hôpital privé Saint-Martin, Pessac
  - Dr Moufid HAJJAR, Cellule d'identitovigilance et de rapprochement du Centre hospitalier universitaire de Bordeaux
  - Mme Marie-Pierre HERRERA, cadre supérieure de santé, Cellule d'identitovigilance et de rapprochement du CHU de Bordeaux
  - Dr Isabelle JAMET, responsable du pôle études, statistiques et évaluation, ARS Nouvelle-Aquitaine
  - Dr Nadia KHALDI, responsable des vigilances, EFS Nouvelle-Aquitaine
  - Dr Jocelyne MONROY, Union régionale des professionnels de santé des médecins libéraux de Nouvelle-Aquitaine
  - Dr Philippe MOREAUD, Union régionale des professionnels de santé des médecins libéraux de Nouvelle-Aquitaine
  - Dr François NASSIRI, Santé-Landes
  - Mme Christelle NOZIERE, GIP ESEA
  - Mme Dany OULEY, ingénieur qualité, Cellule d'identitovigilance et de rapprochement du CHU de Bordeaux
  - Dr Florence PERRET, Département d'information médicale, Maison de santé Marie Galène
  - Dr Jean-Luc QUENON, codirecteur du Centre de coordination de l'évaluation clinique et de la qualité en Nouvelle-Aquitaine (CCECCQA)
  - Dr Catherine RAUTURIER, directeur médical ADAPEI 33
  - Mme Sylvie RIBET, responsable de l'identitovigilance, Groupe Bordeaux Nord Aquitaine
  - Dr Bernard TABUTEAU, pôle qualité et sécurité des soins, ARS Nouvelle-Aquitaine.

SOMMAIRE

NOTES DE VERSION

La première version du référentiel régional d'identitovigilance applicable à la Nouvelle-Aquitaine a été publiée le 26 juin 2017 par le *groupe de travail régional d'identitovigilance* (GTRIV). Les questions qu'elle a suscitées ont fait l'objet de compléments d'informations rassemblées sous la forme de fiches pratiques (cf. 11.3).

A la demande du *comité technique régional d'identitovigilance* (COTRIV) qui a succédé au GTRIV, une mise à jour du référentiel a été réalisée. Elle intègre notamment les données de la version 1 de la *Fiche pratique n° 2 « Foire aux questions »*.

Le plan de la nouvelle version du référentiel régional a été modifié dans un sens plus logique afin de faciliter la lecture et les recherches (cf. 11.2 pour les correspondances entre les 2 versions). Un surlignage signale les principales modifications effectuées dans le texte de la nouvelle version.

Cette mise à jour a été validée le 11 décembre 2018 par le COTRIV.

La version 2 du référentiel régional de bonne pratique devient opposable pour tous les rapprochements d'identités en Nouvelle-Aquitaine à compter du 2 janvier 2019.

1 ENJEUX

La qualité de l'identification d'un usager est l'un des principes fondamentaux de la qualité et de la sécurité de sa prise en charge. Elle doit être le premier acte d'un processus qui se prolonge tout au long de son parcours avec les différents professionnels de santé, quel que soit leur mode d'exercice : libéral ou salarié, en secteur ambulatoire, hospitalier ou médico-social.

Cette exigence est renforcée par les échanges et le partage de données de l'usager au travers de dossiers informatiques (groupements sanitaires, réseaux, dossier médical partagé, dossier pharmaceutique…) ainsi que par leur utilisation potentielle dans le cadre de la télémédecine ou d'objets connectés assurant une surveillance automatisée à distance.

La multiplicité des acteurs concernés, des logiciels, et l'absence de règlementation applicable à tous expliquent qu'il existe des pratiques différentes pour le recueil de l'identité des personnes accueillies et que nombre d'acteurs (professionnels de santé et soignés) ignorent les risques encourus en cas d'identification incorrecte. Les anomalies sont fréquentes, amenant à créer plusieurs dossiers pour un même usager ou, au contraire à fusionner les dossiers d'usagers différents, créant de nouveaux risques liés à la dégradation de la qualité des informations de santé.

La consolidation[1] de l'identité de l'usager est donc un facteur clé de la sécurité de son parcours de santé. La maîtrise des risques dans ce domaine rend nécessaire la définition de règles pertinentes et acceptées par tous : usagers du système de santé, professionnels qui les prennent en charge, mais aussi éditeurs informatiques, assurance maladie et mutuelles.

Il est donc important que tous les acteurs de la santé de la région participent activement à la gestion des risques dans ce domaine : établissements de santé, établissements et structures médico-sociales, plateaux techniques, officines de pharmacie, centres et réseaux de santé, cabinets de ville…

Remarque n° 1 : dans le reste du document les termes suivants seront utilisés de façon générique :
- « structure de santé » pour identifier les professionnels, établissements, services et organismes intervenant dans la prise en charge sanitaire ou médico-sociale ;
- « usagers » au sens des personnes accueillies par ces structures : utilisateurs du système de santé ou personnes accompagnantes.

Remarque n° 2 : les définitions des différents termes techniques soulignés par des pointillés sont précisées en « 10. Glossaire »).

2 POLITIQUE REGIONALE D'IDENTITOVIGILANCE

2.1 Objectifs

La politique menée par l'Agence régionale de santé (ARS) Nouvelle-Aquitaine pour assurer la bonne identification des usagers à toutes les étapes de leur prise en charge sur le territoire poursuit les objectifs suivants :
- améliorer la qualité et la sécurité des prises en charge dans le cadre de la continuité des soins et du partage d'informations entre professionnels intervenant dans un même parcours de santé ;
- définir les principes à appliquer pour l'identification optimale des usagers du système de santé et prévenir, limiter ou corriger les anomalies générées lors de cette étape essentielle ;
- favoriser le respect des bonnes pratiques d'identification des usagers par les professionnels ;

[1] Situation où l'identité est vérifiée et non susceptible de varier (hors modifications futures d'état civil) ; on parle aussi d'identité « certifiée ».

- garantir la confiance dans la qualité des informations échangées entre les systèmes d'information et professionnels de santé ;
- contribuer à l'interopérabilité des systèmes d'information de santé ;
- réduire le risque d'erreurs d'identification des personnes prises en charge ;
- sécuriser le rapprochement d'identité entre structures de santé différentes ;
- encourager le développement d'interfaces logicielles conformes aux exigences en termes d'identitovigilance.

2.2 Périmètre

La politique régionale d'identitovigilance s'applique à tous les modes de prise en charge : hospitalisation, consultation, visite à domicile, télémédecine, accueil dans les établissements et services médico-sociaux…

Les acteurs concernés sont :
- l'usager, acteur de sa sécurité et ses accompagnants : ayant-droit et personne de confiance ;
- 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, sages-femmes, biologistes ;
- les paramédicaux (infirmiers, aides-soignants, psychologues, kinésithérapeutes…) ;
- les secrétaires médicales et assistantes médico-administratives ;
- les ambulanciers et brancardiers ;
- les personnels des services médicotechniques (laboratoire, imagerie, pharmacie à usage intérieur…) ;
- les travailleurs sociaux ;
- les personnels d'accompagnements intervenant au sein des établissements et services médico-sociaux comme ceux intervenant sur le parcours de santé (éducateurs, moniteurs d'ateliers, etc.) ;
- 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…) ;
- les intervenants de sociétés tierces réalisant des prises de rendez-vous par téléphone ;
- les industriels développant des solutions informatiques…

2.3 Gouvernance régionale de l'identitovigilance

2.3.1 Comité de pilotage (COPIL)

Le comité de pilotage (COPIL) de l'identitovigilance est une instance de l'ARS Nouvelle-Aquitaine. Il réunit les responsables de la Direction de la santé publique (DSP) et de la Direction de l'offre de soins et de l'autonomie (DOSA) ainsi que les référents métiers du serveur régional de rapprochement d'Identité (SRI) de l'agence.

Le COPIL a une mission essentiellement stratégique dans le domaine de l'identitovigilance régionale en relation avec les services d'e-santé et la sécurité des parcours de soins : définition de la politique, validation des moyens à mettre en place, évaluation des résultats, avis sur les actions correctrices…

Il se réunit plusieurs fois par an, en fonction des besoins, soit de façon autonome, soit sur sollicitation des référents métiers ARS, du COTRIV ou de la CRIV.

2.3.2 Comité technique régional d'identitovigilance (COTRIV)

Le Comité technique régional de l'identitovigilance (COTRIV) est une instance représentative des professionnels chargés de l'identitovigilance. Il est composé de professionnels de santé volontaires, venus d'horizons différents : représentants d'établissements de santé publics et privés, d'établissements médico-sociaux, de médecins libéraux et d'usagers, de l'Etablissement français du sang, de l'ARS Nouvelle-Aquitaine, du GIP ESEA… Le nombre de professionnels impliqués est susceptible d'évoluer en fonction des besoins et/ou des candidatures reçues et validées par le COTRIV.

Le COTRIV a pour missions de conseiller le COPIL et participer au déploiement de la politique régionale d'identitovigilance. A ce titre, il est notamment chargé de définir les règles régionales d'identification des personnes prises en charge et de produire des outils régionaux favorisant l'appropriation de ces règles et l'harmonisation des pratiques par tous les acteurs de santé prenant en charge des patients ou résidents. Il assure également la veille réglementaire, la mise à jour des outils et la promotion de l'identitovigilance dans la région Nouvelle-Aquitaine. Il sollicite les référents métiers SRI de l'ARS et le COPIL chaque fois que nécessaire.

Il est réuni plusieurs fois dans l'année, en fonction des besoins, sur sollicitation de l'ARS ou de la CRIV. Pour mener à bien ses missions, il peut constituer des groupes de travail ou de réflexion thématiques ayant leur propre calendrier de réunion. Un bilan d'activité est formalisé chaque année

2.3.3 Cellule régionale d'identitovigilance (CRIV)

La Cellule régionale d'identitovigilance (CRIV) a été spécialement créée pour gérer les événements « identitovigilance » en lien avec le SRI. Elle est composée de professionnels de santé référents dans le domaine de l'identitovigilance. Leur nombre et qualifications sont susceptibles d'évoluer en fonction de la charge de travail liée au nombre de structures « raccordées » au SRI et/ou d'événements à gérer. Ils sont membres « de droit » du COTRIV.

Sa mission principale est de piloter la gestion des risques lors du rapprochement des identités dans le SRI en animant le réseau des référents identitovigilance SRI des cellules d'identitovigilance locales. En termes de gestion des risques *a priori*, elle s'assure du respect des exigences régionales des candidats au branchement sur le SRI et donne son avis sur leur éligibilité et/ou les actions à mettre en œuvre pour le devenir. Dans le cadre de la gestion des risques *a posteriori*, elle surveille les différents indicateurs de qualité fournis par le SRI et met si besoin en relation les référents locaux concernés par des identités approchantes entre domaines d'identification différents pour déterminer s'il s'agit ou non de doublons.

Cette mission est assurée pendant les heures ouvrables, selon une organisation précisée aux référents SRI locaux et aux autres instances régionales (COTRIV et COPIL).

2.4 Gouvernance locale de l'identitovigilance

Pour la bonne mise en œuvre de la politique d'identitovigilance dans la structure de santé, il est nécessaire de mettre en place une ou plusieurs instances de gouvernance, adaptée(s) à la taille et à l'activité de la structure.

On peut distinguer :

- un niveau stratégique où se décide la politique à mener en matière d'identitovigilance et les moyens donnés pour y parvenir ;
- un niveau opérationnel chargé du déploiement et de l'évaluation des procédures en vigueur.

2.4.1 Niveau stratégique

La cellule décisionnaire (comité d'identitovigilance, autorité de gestion des identités) a pour missions de définir et suivre :

- la politique d'identitovigilance ;
- la charte d'identitovigilance et les procédures afférentes ;
- la cohérence du système d'information et des interfaces du serveur d'identité avec les applications tierces ;
- la politique de formation et de sensibilisation des acteurs ;
- le système de signalement des dysfonctionnements liés à l'identitovigilance (y compris à l'ARS pour les événements indésirables graves liés au système d'information et les événements indésirables graves associés aux soins) ;
- l'organisation nécessaire à la conduite des actions préventives et correctives en lien avec l'ensemble des parties prenantes, internes et externes, sous l'autorité du référent d'identitovigilance nommé par cette structure ;
- le plan d'actions d'amélioration annuel.

Elle est réunie périodiquement pour analyser les indicateurs de suivi et les anomalies signalées. Un bilan annuel est transmis à la direction de la structure ainsi qu'au *comité technique régional d'identitovigilance* (COTRIV).

2.4.2 Niveau opérationnel

Le niveau opérationnel est le plus souvent dénommé « cellule d'identitovigilance » (CIV). Les professionnels qui la composent sont placés sous l'autorité fonctionnelle du référent local d'identitovigilance. Ils ont pour missions :

- de former les acteurs qui créent ou utilisent des identités, sur la base du plan de formation continue validé par la direction ;
- de sensibiliser l'ensemble des parties prenantes (professionnels, usagers) ;
- de rédiger et/ou actualiser les procédures d'identification primaire de l'usager ;
- de recueillir et analyser les évènements indésirables d'identitovigilance ;
- de réaliser des audits de pratique et audits organisationnels (patient fictif, analyse des barrières de sécurité…) ;
- d'analyser la base de données usagers à la recherche de données manquantes, de doublons, d'erreurs d'identité ;
- de proposer des mesures correctives (dont les rapprochements d'identité et fusions d'identifiants) ;
- de rendre compte de ses activités et difficultés au niveau stratégique.

La CIV se réunit au minimum une fois par trimestre (prérequis *Hôpital Numérique* : indicateur P1.2) et autant que nécessaire en fonction des événements indésirables. Elle réunit la documentation de la politique et du rapprochement d'identité et fournit un rapport périodique d'activité précisant :

- la liste des réunions ;
- les incidents relevés ;
- les corrections et améliorations conduites.

2.4.3 Référent d'identitovigilance

Le référent local d'identitovigilance, désigné par le niveau stratégique, est l'interlocuteur de la structure de santé pour toutes les questions relatives aux bonnes pratiques d'identification des usagers. Il organise et anime les réunions de la CIV et participe aux travaux du niveau stratégique.

Il est en rapport avec ses homologues des structures de santé partageant la prise en charge des mêmes usagers ainsi qu'avec la cellule régionale d'identitovigilance (CRIV) à laquelle il signale les anomalies significatives et les difficultés d'application des règles régionales.

Afin de permettre une cohérence dans le suivi et la gestion des risques des événements indésirables liés à l'identitovigilance, il est recommandé que le référent local travaille en lien étroit avec la cellule qualité/gestion des risques de la structure de santé, ou ce qui en tient lieu.

2.4.4 Correspondants locaux d'identitovigilance

Il peut être utile de disposer de correspondants d'identitovigilance dans les services de soins pour constituer un relais de la CIV au plus près des soignants (informations montantes et descendantes) et participer au déploiement local des actions d'amélioration. Cette mission peut être confiée aux référents qualité et gestion des risques.

2.5 Charte d'identitovigilance

Chaque structure de santé doit décliner la politique institutionnelle d'identification de l'usager au sein d'une charte d'identitovigilance, adaptée à la taille de la structure et à la complexité des prises en charge réalisées. Elle y décrit les moyens mis en œuvre en termes de processus, procédures, ressources humaines et moyens techniques.

La charte a pour objet de formaliser les règles à respecter pour :

- recueillir l'identité exacte des usagers pour chaque domaine d'identification recensé dans la structure ;
- sécuriser les informations médicales en évitant les doublons et collisions ;
- harmoniser et rendre compatibles les procédures locales existantes, préalables indispensables aux rapprochements d'identité inter-structures de santé au niveau régional et donc aux échanges sécurisés de données entre elles.

Les responsables de structures sont invités à créer ou mettre à jour leur charte d'identitovigilance en reprenant les préconisations du présent référentiel, tout en tenant compte des spécificités de l'organisation interne et des systèmes d'information utilisés localement.

L'objectif est que chaque usager soit identifié de manière unique au sein du système d'information de la structure de santé. Cette étape est réalisée en recueillant un certain nombre de « traits » d'identité personnels qui visent à le différencier des autres usagers (cf. 3).

La charte peut s'appuyer sur des procédures annexes qui décrivent précisément certaines activités en relation avec le recueil, le contrôle et l'utilisation de l'identité. La procédure de recueil d'identité définit quels sont les professionnels habilités à saisir une identité, les règles à appliquer pour renseigner les différents traits et assurer leur validation en fonction de la confiance qui peut être accordée aux éléments transmis (informations orales, documents d'identité…). Il peut être nécessaire, selon les besoins de chaque établissement (en fonction de leur activité), d'établir d'autres procédures pour la prise en compte de situations particulières ; par exemple pour définir la conduite à tenir lorsque les éléments de confiance ne sont pas réunis (absence de document officiel d'identité, usager non communiquant) ou dans des cas particuliers où l'usager fait valoir son droit à ne pas être inscrit sous son vrai nom (prise en charge anonyme…).

Des critères doivent permettre de distinguer les identités officielles et vérifiées (sur un document d'identité valide) des identités provisoires ou suspectes, afin qu'il soit possible d'en tenir compte dans les procédures de rapprochement d'identité en interne ou par le biais de serveurs de rapprochement d'identité multi-structures. Il faut notamment tout faire pour éviter les collisions,

c'est à dire la fusion inappropriée de dossiers d'usagers différents car l'opération inverse (dé-fusion) s'avère bien souvent compliquée, voire impossible.

Des instances de gouvernance (comité et/ou cellule d'identitovigilance) sont chargées d'évaluer les pratiques, de recueillir, de traiter les difficultés éventuelles et de faire évoluer les procédures chaque fois que cela se révèle nécessaire. Elles sont à mettre en place au niveau de chaque structure collective, comme à l'échelon régional.

3 VALIDITE DE L'IDENTITE RECUEILLIE

3.1 Niveaux de confiance des documents d'identité

L'identité recueillie doit être évaluée en termes de confiance à accorder en fonction des documents pris en compte lors de l'enregistrement de l'usager dans la base de données.
L'identité ne peut être « **certifiée »** que lorsqu'elle est relevée à partir d'un document d'identité officiel comportant les traits stricts et une photo récente :

- la carte nationale d'identité (CNI) ;
- le passeport ;
- le titre de séjour ;
- l'acte de naissance pour les nouveau-nés.

Elle est à considérer comme « **qualifiée** » lorsqu'elle se base sur d'autres documents officiels :

- le livret de famille, pour les mineurs ne possédant pas de document d'identité ;
- l'extrait d'acte de naissance ;
- le permis de conduire ;
- le document de demandeur d'asile avec photo établi par la préfecture comportant la mention « ce document peut être produit pour toute démarche administrative » ;
- le document de circulation pour étranger mineur délivré par la préfecture.

L'identité ne peut être que **« provisoire »** tant qu'un document officiel d'identité n'a pas été produit. Il est rappelé que les données enregistrées sur la carte Vitale ne sont pas fiables et ne permettent en aucun cas de qualifier l'identité d'un patient. Il en est de même pour les documents de justice qui ne sont pas des pièces officielles d'identité (cf. 4.4.2.2).

Il est recommandé de disposer par ailleurs d'une qualification « **douteux** » pour identifier les cas où l'identité recueillie est suspecte : suspicion d'usurpation d'identité, personne isolée non communicante, langue étrangère non maîtrisée en interne, incohérences entre documents… Ces cas sont à signaler systématiquement à la cellule d'identitovigilance.

Attention : les identités provisoires n'ont pas vocation à être transmises au serveur régional de rapprochement d'identités (SRI).

3.2 Discordances entre documents d'identité

En cas de discordances, c'est le document d'identité ayant le plus fort niveau de confiance qui doit être pris en compte (cf. 3.1). S'il existe des différences entre documents de fort niveau de confiance, il est conseillé d'enregistrer les données de la pièce d'identité la plus récente.

Remarque : Il convient dans tous les cas d'inviter l'usager à faire corriger les données erronées par l'organisme d'état civil compétent.

Après correction, l'établissement est invité à garder une trace des changements d'état civil.

Dans les autres cas, il peut aussi être proposé d'associer plusieurs documents afin d'améliorer le niveau de confiance à accorder, néanmoins **l'identité ne sera pas « certifiée ».**

3.3 Modification des données d'état civil

La rectification des erreurs est un droit que l'usager doit faire valoir auprès du service d'état civil de son domicile ou de son lieu de naissance (art. 60 du code civil modifié par la loi n°2016-1547 du 18 novembre 2016 - art. 56). C'est une procédure gratuite.

Il est également possible de changer gratuitement de prénom sur demande à la mairie et donc de faire officialiser un prénom d'usage en prénom officiel. Pour un mineur, cette modification nécessite l'agrément des 2 parents.

3.4 A savoir

- En termes de validité d'identité, le passeport étranger a plus de valeur qu'un titre de séjour français.
- L'adoption plénière entraîne la modification du nom de naissance, sans lien avec le précédent. En cas d'adoption simple, le nom du ou des adoptants peut s'ajouter ou remplacer le nom de l'adopté
- En France, tout type de requérant peut demander à la mairie du domicile ou du lieu de naissance de lui communiquer les : nom de naissance, prénoms, date et lieu de naissance, ainsi que la dernière situation matrimoniale d'une personne.
- La copie de la pièce d'identité présentée est utile dans la démarche de validation de l'identité, notamment lorsqu'elle est réalisée *a posteriori* par la CIV locale. Il convient toutefois d'être vigilant sur les modalités pratiques de cette opération (insertion dans le dossier papier ou informatique) et la durée de conservation de ce document. La structure de santé doit définir dans une procédure *ad hoc* les conditions de conservation et de destruction de ce type de document. C'est tout particulièrement utile pour la conformité au *règlement général de protection des données* (RGPD) en cas de numérisation intégrée au dossier informatisé.

4 MODELE REGIONAL D'IDENTIFICATION DE L'USAGER

Les données d'identification de l'usager sont réparties en 3 catégories de traits : stricts, étendus et complémentaires.

4.1 Les traits stricts

Ce sont des données stables d'état civil, vérifiables à partir de documents d'identité officiels comportant une photographie (à l'exception de l'acte de naissance et du livret de famille pour les enfants mineurs ne disposant pas de carte d'identité). Une décision de justice peut toutefois modifier certaines de ces données d'où l'intérêt de disposer d'un document d'identité récemment mis à jour en cas de discordance entre les déclarations de l'usager et les données écrites fournies.

Ces données sont obligatoires. Elles sont utilisées comme critères déterminants pour rechercher des dossiers antérieurs ou contribuer à rapprocher des identifiants.

On trouve dans cette catégorie :
- le nom de famille (ou nom de naissance) ;
- le premier prénom de naissance figurant sur le document officiel d'identité (qui peut être composé : cf. 4.4.1) ;
- la date de naissance ;
- le sexe ;
- le lieu de naissance : département, commune et/ou code postal pour un ressortissant français, code PMSI du pays pour un étranger : cf. 11.4).

4.2 Les traits étendus

Ce sont des éléments d'identification supplémentaires qui sont susceptibles de varier dans le temps, au gré des procédures d'état civil (mariage, divorce, adoption…) ou de ne pas être attribués à tous les usagers (jeunes enfants, touristes étrangers, personnes en situation irrégulière).

Ils sont également susceptibles de faciliter les relations avec l'usager utilisant ces traits dans la vie courante (nom d'usage et prénom d'usage, notamment).

Les données peuvent concerner :
- le nom d'usage ;
- le prénom d'usage (officiel ou habituellement utilisé par l'usager) ;
- les autres prénoms de naissance ;
- l'identifiant local attaché à l'usager (ex : IPP) ;
- le NIR personnel ;
- la photographie de l'usager.

4.3 Les traits complémentaires

Ce sont d'autres informations pouvant être utilisées pour faciliter le rapprochement d'identité entre 2 dossiers lorsque les éléments précédents ne sont pas suffisants ou lorsqu'il existe des doutes sur une possible usurpation d'identité.

Pour exemples :
- le NIR de facturation (il peut concerner les différents ayants-droit d'un seul assuré) ;
- l'INS-C (si calculé) ;
- l'adresse de résidence de l'usager ou de l'assuré ;
- les numéros de téléphone ;
- l'adresse courriel de contact ;
- le nom des personnes en relation (parent, enfant, conjoint, personne de confiance…) ;
- le médecin traitant ;
- les autres professionnels de santé impliqués dans la prise en charge ;
- la profession ;
- le document d'identité présenté…

Dans certains cas, il peut être nécessaire de rechercher d'autres traits complémentaires couverts par le secret médical par les professionnels autorisés à consulter le dossier de l'usager ; ils peuvent ainsi émettre un avis positif ou négatif à la fusion de 2 dossiers par la CIV après avoir vérifié la cohérence de données médicales discriminantes telles que la carte de groupe sanguin, le port d'un dispositif médical implantable, la comparaison de paramètres cliniques ou biologiques…

4.4 Cas particuliers

4.4.1 Difficultés relatives au prénom de naissance

4.4.1.1 Prénoms composés

Sur un document d'identité français, une virgule sépare normalement les prénoms.

Le premier prénom peut être composé. Les 2 prénoms sont alors habituellement regroupés par un tiret mais ce n'est pas une règle obligatoire : il est autorisé de porter un prénom composé avec un simple espace de séparation. C'est également le cas pour certains prénoms d'origine étrangère, notamment pour ceux commençant par *Ould*, *Ben* ou *Walid*, qui signifient « fils de », ou ceux composés de mots de liaison tels que : *Dos*, *Das*, *Da*, *Del*, *Della*…

On doit donc enregistrer les prénoms qui apparaissent avant la première virgule, comme « premier prénom de naissance » (cf. 4.1).

Exemples :

- **Avec une virgule on enregistre le(s) prénom(s) précédant celle-ci :**
  - Jean, Pierre, Edouard, Michel ► enregistrer JEAN
  - Jean Pierre, Edouard, Michel ► enregistrer JEAN PIERRE
- **Avec un tiret reliant les 2 premiers prénoms, on enregistre le prénom composé :**
  - Jean-Pierre, Edouard, Michel ► enregistrer JEAN-PIERRE (ou JEAN PIERRE, cf. 5.1)
  - Jean-Pierre Edouard Michel ► enregistrer JEAN-PIERRE (ou JEAN PIERRE, cf. 5.1)
- **En l'absence de virgule, on n'enregistre que le premier prénom de la liste :**
  - Jean Pierre Edouard Michel ► enregistrer JEAN
  - Jean Pierre ► enregistrer JEAN (sauf exception : cf. 4.4.1.2)
- **Quelques exceptions sur des prénoms d'origine étrangère :**
  - Walid, Mahamoud ► enregistrer WALID
  - Ben Mohamed ► enregistrer BEN MOHAMED
  - Ould Ahmed ► enregistrer OULD AHMED
  - Thi Loan ► enregistrer THI LOAN
  - Alcida Dos Anjos ► enregistrer ALCIDA DOS ANJOS

4.4.1.2 Contestation d'enregistrement du premier prénom

S'agissant d'un trait strict, il n'est pas possible de déroger à la règle d'enregistrement du premier prénom de naissance. A défaut de produire un autre document d'identité de haut niveau de confiance permettant de certifier l'identité souhaitée (cf. 3.1), c'est bien celui enregistré sur le document officiel d'identité présenté qui est à enregistrer.

Attention : la possibilité de porter un prénom composé sans tiret de séparation peut parfois poser problème lorsqu'il n'est pas suivi d'une virgule sur la pièce d'identité. Il est alors nécessaire de demander à la personne de prouver l'emploi de ce double prénom dans la vie courante en produisant des documents complémentaires (document juridique, à défaut facture…). C'est donc un traitement au cas par cas qu'il faut apporter à ce type de situation. **Compte tenu de l'interprétation nécessaire, cette identité ne peut être certifiée.**

Exemples :

- Jean Pierre, Edouard ► enregistrer JEAN PIERRE
- Jean Pierre ► enregistrer JEAN (règle générale) ou JEAN PIERRE (avec document preuve)

Remarque : dans les autres cas, l'usager (ou un de ses ayant-droit) doit être invité à faire modifier ses papiers auprès de l'état civil, seule possibilité pour que le changement soit effectivement pris en compte.

4.4.1.3 Enregistrement d'un prénom d'usage

Lorsque le système d'information dispose d'un champ « prénom d'usage » ou dédié à l'enregistrement de traits étendus « autres », il est possible d'enregistrer le prénom habituellement utilisé par l'usager (aux dires de celui-ci) ou indiqué après la mention « prénom d'usage » sur la pièce d'identité.

Dans les autres cas, il doit être ignoré.

4.4.2 Difficultés relatives au nom d'usage

4.4.2.1 Enregistrement du nom d'usage

Le nom d'usage, qu'il soit précédé de « époux/se de », « divorcé/e de », « veuf/ve » (ou leurs équivalents comme « Ep. », « Div. », « Vve ») doit être enregistré tel qu'il apparaît sur le document d'identité présenté dans le champ correspondant (cf. 4.2), sans la mention qui le précède.

Remarque : il n'y a pas lieu de recopier le nom de famille (nom de naissance) dans le champ « nom d'usage » sauf si cette opération est requise par le logiciel utilisé. Il ne peut donc s'agir que d'une consigne locale, inscrite dans la charte d'identitovigilance de la structure (cf. 5.4).

4.4.2.2 Contestation d'enregistrement du nom d'usage

Certaines personnes divorcées présentent des documents d'identité mentionnant encore le nom de l'ex-conjoint, soit parce que c'est un choix fait lors du divorce (avec l'accord de l'ex- conjoint), soit parce que la pièce d'identité n'a pas été mise à jour. L'enregistrement des identifiants est à réaliser sans déroger à la règle générale, en recopiant les mentions portées sur la pièce d'identité présentée.

En cas de contestation, il appartient à l'usager de présenter un document d'identité de haut niveau de confiance (cf. 3.1) ou, à défaut, une décision de justice.

Si une décision de justice est présentée et qu'il y est fait référence d'un changement de statut marital, comme par exemple un divorce, il est possible de ne pas faire apparaitre le nom d'usage mais l'identité ne pourra pas être certifiée tant qu'une pièce d'identité officielle corrigée n'aura pas été présentée.

Attention : dans tous les cas, il faut inviter les contestataires à mettre à jour, dès que possible, ses documents auprès de l'état civil ; seule possibilité pour que le changement soit effectivement pris en compte par la structure.

4.4.3 Identités sensibles

Certaine identités doivent être traitées de manière spécifique de façon à garantir leur confidentialité. C'est le cas par exemple des hospitalisations « sous X », des détenus… Elles doivent donc faire l'objet de procédures internes qui en précisent les modalités pratiques (cf. 7).

Attention : ces identités n'ont pas vocation à être transmises au serveur régional de rapprochement d'Identités (SRI).

4.4.4 Certificats de décès

Les règles d'identitovigilance sont également importantes à respecter lors de la rédaction des certificats de décès. Il est tout particulièrement important de vérifier que les données remplies automatiquement par voie informatique correspondent bien aux champs attendus en évitant, par exemple, que le nom d'usage soit renseigné à la place du nom de famille…

4.5 Difficultés d'application du référentiel

On peut trouver sur certaines pièces d'identité des mentions qui dérogent aux règles établies dans le référentiel régional et/ou avoir des difficultés d'interprétation des documents fournis, dans ce cas :

- consulter la fiche pratique de recueil des identités françaises et étrangères (cf. 11.3.1) en première intention ;
- prendre contact avec la CRIV (adresse mail : criv@sri-na.fr).

5 REGLES POUR LA CREATION D'UNE IDENTITE

L'instruction DGOS/MSIOS du 7 juin 2013, relative à l'identification des patients, fixe un certain nombre de règles strictes à appliquer par les structures de santé. Cette instruction n'est toutefois pas opposable à toutes les structures (comme les EFS) et ne peut être appliquée par tous au regard des contraintes des systèmes d'information de chaque établissement.

Les règles à appliquer en Nouvelle-Aquitaine sont celles retenues par le Comité technique régional d'identitovigilance (COTRIV). Elles sont détaillées ci-après.

5.1 Utilisation des tirets et apostrophes

A l'exception des accents, il est demandé de recopier de façon la plus fidèle possible les traits stricts tels qu'ils sont enregistrés sur les documents d'identité présentés.

Remarque : la consigne donnée par la DGOS de remplacer tirets et apostrophes par des espaces n'avait été édictée que pour faire face à l'incompétence de certains logiciels à traiter ces caractères dans les opérations de recherche et de rapprochement. La plupart des logiciels métiers ont évolué et sont capables, aujourd'hui, de remplacer virtuellement les caractères de ponctuation (apostrophes, tirets, parenthèses) par des espaces lors de ces opérations, ce qui rend obsolète cette règle dans la plupart des cas. C'est notamment le cas du serveur régional de rapprochement d'identités (SRI).

Il est donc permis aux établissements de choisir la méthode d'enregistrement la plus appropriée selon les exigences de leur système d'information :

- soit de recopier le plus fidèlement possible les traits des documents présentés, méthode préconisée par le référentiel, lorsque le système d'information est en capacité de supprimer ces caractères lors d'opérations de recherche et de rapprochement ;
- soit de les remplacer par des espaces, comme le propose l'instruction, dans le cas où la configuration locale n'offre pas de possibilité de paramétrage avancé de ces opérations.

Exemples :

- Jean-Pierre → JEAN-PIERRE (méthode 1) ou JEAN PIERRE (méthode 2)
- O'BRIEN → O'BRIEN (méthode 1) ou O BRIEN (méthode 2)

Remarque : une fois la méthode choisie, elle ne doit pas être changée sans en évaluer les conséquences au préalable, notamment pour les patients déjà inscrits dans la base de l'établissement.

5.2 Transcription des caractères spéciaux

La règle est de transformer les caractères alphabétiques spéciaux en version non accentuée.

- Exemples : È → E ; Ø → O ; Å → A ; Ü → U ; Œ → OE ; etc.
- Cas particulier : ß (*eszett* allemand) → SS

Remarque : cette règle prévaut même si la zone codée en bas du document de certains pays comporte une traduction phonétique différente. Par exemple : MŰLER, codé MUELER en bas d'un passeport Bulgare, est à enregistrer comme MULER.

5.3 Règles particulières concernant les traits stricts

- En l'absence de prénom, il faut saisir les informations telles qu'elles apparaissent sur le document d'identité (exemples : XX, SP, SANS PRENOM) ;
- Si le **jour de la naissance** est inconnu, on enregistre par défaut « **01/MM/AAAA** ».
- Si le **mois** n'est pas connu, on enregistre par défaut le mois de janvier « **JJ/01/AAAA** ».
- Si le **jour et le mois** ne sont pas connus, on enregistre par défaut la date du 31 décembre de l'année de naissance[2] : « **31/12/AAAA** »
- Si l'**année** n'est pas connue précisément, on enregistre par défaut la décennie : **JJ/MM/AAA0**
- Il en résulte que pour une **date de naissance inconnue**, on enregistre **31/12 et une décennie** compatible, par exemple, 31/12/1970 (cf. *Instruction générale relative à l'état civil du 2 novembre 2004*).
- En présence d'une discordance entre les données d'identité officielles et celles enregistrées par l'assurance maladie, il faut saisir dans les traits stricts les éléments indiqués sur le document d'identité. Les éléments discordants portés par la carte Vitale ne doivent être saisis que s'il existe des champs spécifiques dans le système d'information permettant de préciser ces différences dans les données de sécurité sociale.
- La nécessité de tronquer un nom faute d'espace suffisant devrait être signalée afin d'en tenir compte lors des opérations de rapprochement.
- Des procédures dégradées sont à définir par les structures de santé en cas d'absence d'information sur certains traits stricts (par exemple lieu de naissance inconnu).

5.4 Règles particulières concernant les traits étendus

L'utilisation du nom d'usage et/ou du prénom d'usage peut être utile pour les rapports avec les usagers au cours de leur prise en charge ; s'ils sont différents du nom de famille et du prénom de naissance, ils ne doivent en aucun cas être saisis dans les traits stricts mais enregistrés dans les traits étendus, charge à l'établissement de définir comment faire apparaître ces données dans les pièces du dossier de l'usager, sans risque d'erreur avec les traits stricts (cf. 6.4)

Pour les structures de santé qui disposent d'un logiciel rendant obligatoire la saisie d'un nom d'usage, pour les usagers qui n'en disposent pas, il faut recopier le nom de famille (naissance) dans ce champ (cf. 4.4.2.1).

[2] Consigne non applicable pour des enfants de moins d'1 an hospitalisés (date d'entrée de prise en charge est antérieure à la date de naissance). En l'absence de précision sur ce point au niveau national, on peut recommander d'estimer approximativement le mois de naissance (01/mm/aaaa).

6 REGLES D'APPLICATION EN MATIERE D'IDENTITOVIGILANCE

La qualité des données qui composent la base de données des usagers est primordiale. Les structures de santé doivent mettre en œuvre des procédures destinées à fiabiliser l'identification des usagers et à maintenir la qualité des données, en particulier pour :

- les usagers dans l'incapacité de décliner leur identité ;
- les usagers souhaitant garder l'anonymat ;
- les usagers ayant une identité d'emprunt...

6.1 Référentiel d'identité

Au sein d'une structure de santé, le système d'information (SI) intègre les applications de gestion administrative et de processus de soins indispensables à la traçabilité des données de prise en charge.

Chaque structure de santé doit disposer d'un référentiel unique d'identités. C'est un ensemble de composants (techniques et organisationnels) du SI qui garantit la cohérence des données d'identité pour l'ensemble des logiciels métiers gérant des informations nominatives des personnes prises en charge.

6.2 Recueil de l'identité

L'enregistrement de l'identité de l'usager dans le SI est réalisé sous la responsabilité de professionnels habilités en interne à le faire (cf. 6.5.2). Cette opération est réalisée après contrôle immédiat ou secondaire des documents d'identité (cf. 3).

6.3 Recherche dans la base

Afin d'éviter la création de doublons et la survenue de collisions, la recherche de l'enregistrement d'un usager dans la base de données est impérative avant toute création d'un nouvel identifiant.

La recherche se fait prioritairement par la date de naissance et peut être affinée si besoin par la saisie de critères de recherche supplémentaires sur d'autres traits stricts. Par exemple :

- renseigner la date de naissance
- entrer les 3 premières lettres du nom (famille ou usage en fonction du SI) suivi, si besoin, d'un caractère spécial complétant la recherche (ex : %).

Attention : en aucun cas l'identité complète (nom, prénom, date de naissance) ne doit être renseignée à l'étape de recherche.

6.4 Règles d'impression des documents comportant une identité

Toutes les pièces du dossier d'un usager doivent être identifiées avec, au minimum, le nom de famille (naissance), le sexe, le prénom et la date de naissance. Il est recommandé d'y ajouter le nom d'usage à condition qu'il soit bien identifié comme tel.

Remarque : cette recommandation n'est bien sûr pas applicable dans toutes les situations où s'appliquent des droits particuliers en termes de gestion des identités sensibles (cf. **Erreur ! Source u renvoi introuvable.**). Les procédures (cf. 7) sur lesquelles s'appuie ce type de prise en charge doivent préciser les règles d'identification des documents à adopter.

Il faut être particulièrement attentif aux données portées sur les étiquettes et documents imprimés par les différents intervenants habilités à le faire (admissions, secrétariat, service de soins, plateau technique…) afin que soit bien distingué :

- ce qui relève des traits stricts (en distinguant le nom du prénom),
- ce qui relève des traits étendus.

Il est important de vérifier qu'aucune ambiguïté n'est possible, notamment dans les échanges entres structures différentes. Il faut pour cela préciser le nom du champ correspondant, sans équivoque possible : soit de façon explicite, soit de façon abrégée. Pour exemples :

Trait	*Nom du champ explicite*	*Nom du champ abrégé*
Nom de famille	Nom naissance :	N.Nais :
Date de naissance	Date naissance :	DDN :
Sexe	Sexe :	S :
Prénom[3]	Prénom :	Pr. :
Nom d'usage	Nom usage :	N.Us :

Toute anomalie doit être signalée à la (aux) cellule(s) d'identitovigilance concernée(s) pour mise en œuvre des actions correctives.

Une procédure des modalités à suivre dans le cas d'une anomalie constatée concernant l'identité d'un usager provenant d'une autre structure (cf. 7.2.1), doit être mise en œuvre afin d'informer la (ou les) structure(s) concernée(s).

6.5 Sécurité du système d'information

6.5.1 Procédure

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, est élaborée au sein de l'établissement. Elle est diffusée au personnel et aux nouveaux arrivants.

Remarque : dans le cadre de la certification V2014, les prérequis du programme « Hôpital Numérique », s'imposent à tous les établissements de santé. Une partie des indicateurs décline notamment les attendus en termes de fiabilité, de confidentialité, de sécurité et de traçabilité du système d'information.

6.5.2 Droits de création et modification d'identité

Les droits de création et de modification d'identité dans le système d'information doivent être réservés à un nombre limité de professionnels. 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, urgences, secrétariat médical….

La politique d'habilitation et les droits individuels attribués aux professionnels doivent être formalisés dans un document qualité adapté (cf. 7.1.1).

6.5.3 Droits de rapprochement et fusion

La possibilité de faire une fusion ne doit être attribuée qu'à des membres spécialement désignés de la CIV. Les droits individuels doivent être tracés dans un document qualité adapté (cf. 7.1.2).

[3] Il s'agit du premier prénom de naissance, comme précisé dans les traits stricts.

La structure de santé prend les dispositions nécessaires pour organiser la réalisation des fusions dans les logiciels tiers lorsque la fusion n'est pas intégrée automatiquement (cf. 7.1.3).

Les opérations doivent être tracées (historisation informatique ou consigne manuelle).

6.5.4 Confidentialité

Les niveaux d'habilitation d'accès aux différentes applications sont tracés dans un document qualité adapté. Ils sont validés par le niveau stratégique local d'identitovigilance.

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 aux dossiers, qu'ils soient numériques (réseau et logiciels) ou physiques (papier), est strictement limité à ceux des usagers dont le professionnel contribue à assurer la prise en charge.

Les accès aux données de santé numériques par les professionnels doivent être enregistrés et horodatés. Il faut prévoir des précautions particulières lorsqu'un professionnel accède à des données d'un patient qu'il ne prend pas directement en charge.

6.5.5 Référents logiciels

Un référent (au moins) doit être nommé pour chaque logiciel métier participant à la prise en charge de l'usager.

7 PROCEDURES

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

Pour exemples :

- Identification primaire à l'accueil de l'usager dans la structure ;
- Identification secondaire d'un usager avant tout acte de soin ;
- Identification provisoire de l'usager en situation d'urgence ;
- Enregistrement d'un usager incapable de donner ou justifier son identité ;
- Identification des victimes lors de situation sanitaire exceptionnelle (afflux massif);
- Admission d'un usager souhaitant garder l'anonymat ;
- Utilisation d'un bracelet d'identification ;
- Recherche d'un usager dans la base ;
- Contrôle qualité des bases d'identités ;
- Correction et rapprochement d'identités (et/ou fusion) ;
- Gestion d'une suspicion d'usurpation d'identité ;
- Gestion de l'identification primaire et secondaire en cas de panne du système d'information ;
- Gestion des identités dans les logiciels non ou incomplètement interfacés.
- Gestion des homonymes.

7.1 Modification et rapprochement d'identité

7.1.1 Modification d'identité

La modification d'identité n'est autorisée que pour des personnels habilités de la structure de santé (cf. 6.5.2). Elle est décrite dans une procédure spécifique.

Elle ne peut être réalisée qu'au vu d'un document d'identité officiel (cf. 3), conformément à la procédure du recueil de l'identité. Le système d'information doit, de préférence, garder une trace de la modification effectuée (« historisation ») ainsi que de la qualification du niveau de confiance à accorder à la nouvelle identité.

Attention : après modification d'identité, il faut s'assurer que l'information est transmise à tous les acteurs concernés, internes et externes à la structure, et que l'ensemble des pièces du dossier comportent bien la nouvelle identité.

7.1.2 Rapprochement dans le domaine d'identification (fusion)

La fusion de dossiers sous un même identifiant n'est autorisé que pour des personnels spécialement habilités (cf. 6.5.3), sous le contrôle de la CIV. Elle est décrite dans une procédure spécifique.

Le système d'information doit de préférence garder une trace de la modification effectuée (« historisation »).

Attention : après fusion des identifiants, il faut s'assurer que l'information est transmise à tous des acteurs concernés, internes et externes à la structure, et que l'ensemble des pièces du dossier comportent bien le bon identifiant.

7.1.3 Rapprochement dans les logiciels périphériques

Il peut être nécessaire d'appliquer en cascade la fusion réalisée dans le domaine d'identification dans les logiciels non directement interfacés avec le serveur d'identité. Elle doit faire l'objet d'une procédure spécifique et confiée aux référents des logiciels métiers concernés (cf. 6.5.5).

7.1.4 Identification des homonymes

La notion d'homonymie est définie comme la correspondance exacte entre plusieurs traits stricts (décrits au 4.1).

La détection d'homonymes doit conduire à identifier formellement ce statut dans la base d'identité pour faciliter la vigilance des parties prenantes lors d'une venue. Des caractères déterminants doivent être définis pour distinguer les différents homonymes de la base (ex : indexation, ajout des autres prénoms…). Il peut également être utile de faciliter l'accès aux dossiers des homonymes correspondants pour améliorer leur gestion.

Attention : lors de l'arrivée d'un patient ayant des homonymes, il est important de prévoir comment diffuser une alerte aux différents correspondants (laboratoire, service d'imagerie, EFS…) pour limiter le risque d'erreur : contact téléphonique, alerte par message, étiquetage spécifique, etc.

7.2 Identification secondaire

7.2.1 Identification de l'usager lors d'un acte de soins

Les modalités de sécurisation de l'identification secondaire des usagers lors de la réalisation d'un soin par un professionnel sont à définir dans la charte d'identitovigilance (cf. 2.5) ou dans une procédure spécifique. Elles concernent par exemple :

- les questions ouvertes à poser pour vérifier l'identité d'une personne (qui, quand, comment) ;
- l'utilisation pratique des bracelets d'identification lorsque leur utilisation est prévue.

Attention : une procédure doit préciser les modalités à suivre en cas de constatation d'anomalie relative à l'identification.

7.2.2 Dispositifs d'identification physique

Plusieurs dispositifs peuvent participer à l'identification des patients tels que la pose d'un bracelet, l'utilisation d'une photographie dans le dossier patient.

L'emploi d'un dispositif d'identification est 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 dommageable ou préjudiciable (biopsie, endoscopie, imagerie interventionnelle, chimiothérapie, traitement allergisant…) ;
- nouveaux nés ;
- avec lesquels la communication est difficile : non francophone, patient incapable de parler, confus, inconscient, dément…
- décédés, non porteurs d'un bracelet au cours de leur séjour, en vue de leur transfert en chambre mortuaire…

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

- l'information de l'usager, de sa famille ou de sa personne de confiance (le plus souvent, l'accord est tacite) ;
- les modalités de préparation, de pose et dépose du bracelet ou de mise à jour de la photographie ;
- les modalités pratiques d'utilisation ;
- la conduite à tenir en cas de refus de ce type d'identification ou de nécessité de dépose du bracelet en cours de séjour, qu'elle qu'en soit la raison…

Il faut éviter la transcription manuelle de l'identité de l'usager sur le bracelet (source d'erreurs) et privilégier les bracelets comportant une identité imprimée à partir des données informatisées (cf. 6.4).

7.2.3 Identification des documents du dossier de l'usager

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, document de transfert…) soient identifiés sur toutes les pages par, au minimum, les traits stricts (cf. 6.4).

De même, il doit exister une procédure qui précise les modalités pratiques de numérisation et d'identification des documents numérisés joints au dossier informatique de l'usager afin de limiter le risque d'erreur d'attribution.

Remarque : si les documents fournis par le patient ne sont pas correctement identifiés, il est recommandé de coller une étiquette interne (cf. 6.4) en veillant à ce que celle-ci ne recouvre pas les données d'identité initiales du document.

8 FORMATION ET SENSIBILISATION A L'IDENTITOVIGILANCE

8.1 Formation du personnel

La formation et la sensibilisation du personnel qu'il soit administratif ou technique, médical ou paramédical, doivent être prévues par la structure de santé et prendre en compte tous les aspects de l'identitovigilance.

Elle doit aussi concerner les intervenants externes : ambulanciers, professionnels et structures adressant des usagers, plateaux techniques…

Attention : il est nécessaire de s'assurer que les personnels maîtrisent les applicatifs qu'ils utilisent et les procédures dégradées éventuelles (évaluations).

8.2 Sensibilisation des usagers

Les usagers et les accompagnants doivent être sensibilisés à l'identitovigilance, notamment par voie d'affichage et au travers du livret d'accueil. Ils doivent être incités à participer à leur identification et à vérifier les informations utilisées pour les identifier.

8.3 Respect des droits des usagers

Les structures de santé respectent les principes des chartes des usagers hospitalisés.

Ces chartes rappellent les droits des usagers qui sont notamment :
- d'être informé en cas de traitement automatisé des informations les concernant ;
- d'avoir accès aux informations médicales les concernant ;
- de demander la rectification des données erronées ou périmées ;
- d'avoir la garantie de la confidentialité des informations les concernant…

Une attention toute particulière doit être portée à la communication réalisée auprès des usagers (affichage, livret d'accueil…), qui doit leur permettre de comprendre l'importance de l'Identitovigilance, pour leur propre sécurité.

Par ailleurs, les usagers doivent être informés au plus tôt des documents qui leur seront réclamés tout au long de leurs prises en charge programmées (document d'identité officiel notamment).

9 INDICATEURS QUALITE

Les indicateurs qualité ont pour but d'évaluer la performance du système.

Deux types d'indicateurs doivent être suivis :
- Les indicateurs portant sur l'identification primaire des usagers ;
- Les indicateurs portant sur l'identification secondaire des usagers.

Une liste non exhaustive d'indicateurs est proposée ici :
- Taux de doublons ;
- Nombre de fusions ;
- Nombre de collisions détectées ;
- Nombre de dé-fusions ;
- Taux de modifications d'identité ;
- Proportions d'identité certifié/qualifié/provisoire ;
- Nombre d'usurpations d'identités détectées ;
- Taux de fiches de signalement d'événements indésirables (FSEI) relatives à l'identification primaire des usagers ;
- Taux de FSEI relatives à l'identification secondaire des usagers ;
- Indicateurs pour l'amélioration de la qualité et de la sécurité des soins (IPAQSS) du thème « Tenue du dossier patient » ;
- Taux de formation du personnel à l'identitovigilance…

10 GLOSSAIRE

10.1 Collision

La collision correspond à l'attribution d'un même identifiant à 2 personnes différentes, ou plus. Il devient très difficile dans ce cas de faire la part *a posteriori* des informations médicales qui relèvent de chaque usager. Le risque est de prendre des décisions médicales et soignantes au regard des données de santé d'une autre personne.

10.2 Dé-fusion

Elle correspond à l'opération inverse de la fusion en cherchant à réattribuer à chaque usager concerné par une collision, sous un identifiant personnel, les données qui lui sont propres.

10.3 Domaine d'identification

Le domaine d'identification regroupe, au sein d'une organisation ou d'un réseau de santé, toutes les applications qui utilisent le même référentiel d'identité patient pour désigner un usager. Pour exemples : un établissement, un groupement de structures, un cabinet médical.

10.4 Domaine de rapprochement

Un domaine de rapprochement rassemble plusieurs domaines d'identification qui échangent des informations entre eux. Pour exemple, dans un établissement de santé, les identités sont corrélées à un identifiant permanent du patient (IPP) ; tous les logiciels qui l'exploitent font partie du même domaine d'identification. Les logiciels qui utilisent un identifiant interne différent constituent un domaine d'identification distinct. Les échanges entre ces domaines est assuré au sein du domaine de rapprochement qui peut être local ou non.

10.5 Doublon

On parle de doublon d'identités lorsqu'une même personne est enregistrée sous 2 identifiants différents (ou plus) dans une même base de données ; on dispose alors pour l'usager de plusieurs dossiers médicaux et administratifs différents qui ne communiquent pas entre eux. Le fait de ne pas disposer de l'ensemble des informations médicales concernant l'usager engendre un risque lié à la méconnaissance, par le professionnel, de données utiles à la prise de décision.

10.6 Etat civil

En droit français, l'état civil est constitué des éléments qui permettent l'identification d'une personne, tels que le nom, le ou les prénoms, le sexe, la date et le lieu de naissance, la filiation, la nationalité, le domicile, la situation matrimoniale, la date et le lieu de décès. Toute personne vivant habituellement en France, même si elle est née à l'étranger et possède une nationalité étrangère, doit être pourvue d'un état civil.

10.7 Fusion

Elle correspond au transfert, sur un identifiant unique, de toutes les informations dispersées sur plusieurs identifiants (doublons).

10.8 Homonymie

La notion d'homonymie est définie comme la correspondance exacte entre plusieurs traits stricts (cf. 7.1.4).

10.9 Identifiant

Il correspond au code alphanumérique utilisé par un ou plusieurs systèmes d'information pour représenter une personne physique. Pour exemples : identifiant permanent du patient (IPP), identifiant national de santé (INS)…

10.10 Identifiant national de santé (INS)

L'ouverture d'un dossier médical partagé (DMP) suppose l'obtention préalable d'un identifiant national de santé (INS).

Un INS calculé (INS-C), attribué au travers d'un algorithme à partir d'informations lues dans la carte Vitale de l'assuré, a été utilisé pour éviter l'utilisation du numéro de sécurité sociale. Les modalités de calcul de l'INS-C s'étant révélées à l'origine de doublons ou de collisions, il a finalement été décidé de retenir le NIR comme identifiant national de santé (cf. 10.14).

10.11 Identification

C'est l'opération consistant à attribuer de manière univoque à une personne physique une identité qui lui est propre. Dans un système d'information, elle correspond au rattachement à un identifiant existant ou à la création d'un nouvel identifiant.

On distingue :

- **l'identification primaire**, qui correspond à la vérification de l'identité pour l'attribution d'un identifiant dans le système d'information (en le créant ou en utilisant un identifiant déjà présent dans la base).
- **l'identification secondaire**, qui correspond à la vérification par tout professionnel de santé, de l'identité de l'usager avant la réalisation d'un acte le concernant (prélèvement, soins, transport), lors de l'étiquetage des prélèvements ou des documents de l'usager, ou lors de la sélection du dossier usager dans une application (prescription, dossier de soins, suivi médical…).

10.12 Identité

Ensemble de données qui constitue la représentation d'une personne physique. Elle est composée d'un profil de traits. Pour l'identification primaire de l'usager dans les systèmes informatiques, l'identité est associée à un identifiant.

10.13 Interopérabilité de systèmes informatiques

Capacité de ces systèmes à réaliser des opérations compatibles et/ou coordonnées, et à échanger des informations.

10.14 NIR, NIA

Le numéro d'inscription au répertoire des personnes physiques (NIRPP ou NIR), encore appelé « numéro de sécurité sociale », sert à identifier une personne dans le répertoire national

d'identification des personnes physiques (RNIPP). Il est réputé comme « identifiant fiable et stable, conçu pour rester immuable la vie durant ».

Le NIR constitue l'identifiant national de santé (INS) des personnes prises en charge dans les champs sanitaire et médico-social (articles L.1111-8-1, R.1111-8-1 et suivants du code de la santé publique). Un référentiel, publié avant le 31 mars 2018, en définira les modalités de mise en œuvre, dispensant alors les utilisateurs habilités à déclarer son utilisation auprès de la CNIL (Décret n° 2017-412 du 27 mars 2017, article 2).

Le NIR est attribué :

- soit par l'INSEE lors de l'inscription au RNIPP ; l'inscription a lieu, en général, au plus tard huit jours après la naissance, à partir de l'état civil transmis par les mairies (sexe, année et mois de naissance, département et commune de naissance, numéro d'ordre du registre d'état civil) ;
- soit par la CNAVTS lors de l'inscription sur le système national de gestion des identités (SNGI) à la demande d'un organisme de sécurité sociale (CARSAT, CPAM, CAF, MSA, RSI, etc.), à l'occasion d'une démarche effectuée par la personne elle-même ou par son employeur.

Les deux systèmes sont synchronisés quotidiennement.

Pour les personnes nées à l'étranger, il est attribué un NIA, numéro identifiant d'attente attribué par la CNAVTS à partir des données d'état civil (art. R.114-26 du code de la sécurité sociale). Le NIA devient NIR lorsque l'identité de la personne est confirmée (la structure du NIA est la même que celle du NIR).

La fourniture du NIR/NIA doit être assurée par la CNAVTS au plus tard le 31 décembre 2018. Les professionnels habilités pourront y accéder à partir de la carte Vitale ou, lorsque cette information n'est pas disponible, au moyen des services de recherche et de vérification de l'identifiant de santé mis en œuvre par la CNAMTS.

Les professionnels de santé et les établissements auront un an à compter de cette date pour se mettre en conformité. Il ne sera alors plus possible d'utiliser un autre identifiant, sauf en cas d'impossibilité de pouvoir accéder au NIR.

Remarque : les personnes de passage (touristes par exemple) ne se voient pas attribuer de NIR.

10.15 Nom de famille

Le terme « nom de famille » a succédé à celui de « nom patronymique » ou « nom de naissance » ou « nom de jeune fille ». Il est transmis selon des règles propres à la filiation. Il est toujours intégré dans l'extrait d'acte de naissance.

Le changement de nom est prévu par les articles 60 à 62-4 du code civil. Il peut être lié à la procédure de francisation du nom et/ou des prénoms pour les personnes qui acquièrent ou recouvrent la nationalité française.

10.16 Nom d'usage

Il correspond en général au « nom marital » dont la mention peut être portée sur un document officiel comme la carte d'identité. Sur la carte d'identité, il est précisé sous la rubrique « Nom » après « Nom d'usage », « Époux(se) » ou « Veuf(ve) ».

10.17 Prénom de naissance

L'attribution d'un prénom est obligatoire : il est indiqué sur l'acte de naissance. Lorsqu'il en comporte plusieurs, c'est le premier prénom qui sert de prénom de naissance : il est celui qui apparaît avant la virgule sur la carte d'identité (cf. 4.4.1).

Remarques :
- Sur les documents anciens (cartes nationales d'identité émises avant 1995, passeports avant 2001), la liste des prénoms peut être mentionnée sans utilisation de la virgule.
- Le tiret est en principe utilisé pour le prénom composé mais ce n'est pas obligatoire.

10.18 Prénom d'usage

Tout prénom inscrit dans l'acte de naissance peut être choisi comme prénom usuel (art. 57 du code civil), ce choix est alors précisé après la mention « Prénom d'usage » en dessous la rubrique « Prénom(s) » de la carte d'identité.

En termes d'identitovigilance, il ne remplace pas le premier prénom du document d'identité (cf. 4.4.1) et ne peut être enregistré que dans les systèmes d'information qui dispose d'un champ spécifique (cf. 4.4.1.3).

10.19 Pseudonyme

Nom d'emprunt ou « alias » librement choisi par une personne pour dissimuler son identité réelle dans l'exercice d'une activité particulière, notamment dans le milieu littéraire ou artistique. Il ne fait l'objet d'aucune réglementation particulière et ne peut être mentionné sur les actes d'état civil. Un pseudonyme peut toutefois figurer sur la carte d'identité si sa notoriété est confirmée par un usage constant et ininterrompu.

Il est précédé de la mention « Pseudonyme » ou de l'adjectif « dit » sur une ligne spécifique.

Ex : « Dit : Johnny Hallyday »

Remarque : il ne peut être renseigné que dans les cas où le système d'information dispose d'un champ permettant l'enregistrement de traits étendus divers, au même titre que le prénom d'usage.

Attention : le mot « dit » est parfois inclus dans la ligne du nom. Il est alors considéré comme faisant partie complète du nom à enregistrer

10.20 Rapprochement d'identité

C'est une opération qui consiste à mettre en correspondance, pour une même personne, 2 identités provenant de 2 domaines d'identification différents (ou plus). Le rapprochement peut être réalisé entre 2 établissements, 2 applications d'un même établissement…

10.21 Surnom ou sobriquet

Il peut être mentionné sur l'acte de naissance si une confusion est à craindre entre plusieurs homonymes ; en pareil cas, il est précédé de l'adjectif « dit ». Il doit être enregistré comme partie intégrante du nom s'il est précisé sur la même ligne. Ex : « Dupond dit Martin ».

10.22 Traits

Ce sont des éléments d'informations propres à un usager, d'importance variable : « stricts », « étendus » ou « complémentaires ».

Un « profil de traits » correspond à l'ensemble des caractéristiques qui permettent de décrire une personne physique de manière univoque.

10.23 Usurpation d'identité

Action volontaire d'un individu visant à utiliser l'identité d'une autre personne, notamment dans le but de bénéficier de sa couverture sociale.

L'usurpation d'identité peut engendrer des risques très graves pour la santé de l'usurpateur mais aussi du titulaire des droits lors d'un prochain séjour dans l'établissement de soins par le mélange des informations qu'elle entraîne dans le même dossier.

11 ANNEXES

11.1 Références réglementaires et techniques

- Loi n° 2002-304 du 4 mars 2002 relative au nom de famille
- Instruction générale relative à l'état civil du 2 novembre 2004
- Circulaire du 28 juin 1986 relative à la mise en œuvre de l'article 43 de la loi n° 65-1372 du 23 décembre 1985. Usage du nom du parent qui n'est pas transmis. Dénomination des personnes dans les documents administratifs.
- Circulaire du 28 octobre 2011 relative aux règles particulières à divers actes de l'état civil relatifs à la naissance et à la filiation
- Instruction N° DGOS/MSIOS/2013/281 du 7 juin 2013 relative à l'utilisation du nom de famille (ou nom de naissance) pour l'identification des patients dans les systèmes d'information des structures de soins.
- Circulaire n° INT/D/00/00001/C du 10 janvier 2009 relative à l'établissement et la délivrance des cartes nationales d'identité.
- La loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle
- Guide méthodologique Mise en œuvre de l'identité patient au sein des groupements hospitaliers de territoire (ASIP Santé, 2018)

11.2 Correspondance entre les chapitres des 2 versions du référentiel

Chapitres de la v1	Correspondance en v2
1 ENJEUX	1
2 POLITIQUE REGIONALE D'IDENTITOVIGILANCE	2
2.1 Objectifs	2.1
2.2 Périmètre	2.2
2.3 Gouvernance régionale de l'identitovigilance	2.3
2.4 Charte d'identitovigilance	2.5
2.5 Modèle régional d'identification de l'usager	4
3 GESTION DES RISQUES EN MATIERE D'IDENTITOVIGILANCE	6
3.1 Référentiel d'identité	6.1
3.2 Recueil de l'identité	6.2
3.3 Validation de l'identité	3
3.4 Recherche dans la base	6.3
3.5 Règles de saisies pour la création d'une identité	5
3.6 Règles d'impression des documents comportant une identité	6.4
3.7 Gouvernance locale de l'identitovigilance	2.4
3.8 Sécurité du système d'information	6.5
4 PROCEDURES	7
4.1 Modification et rapprochement d'identité	7.1
4.2 Identification secondaire	7.2
5 FORMATION ET SENSIBILISATION A L'IDENTITOVIGILANCE	8
5.1 Formation du personnel	8.1
5.2 Sensibilisation des usagers	8.2
5.3 Respect des droits des usagers	8.3
6 INDICATEURS QUALITE	9
7 ANNEXES	11
7.1 Références réglementaires et techniques	11.1
7.2 Glossaire	10

11.3 Fiches pratiques (FP)

11.3.1 FP 1 : Recueil de l'identité à partir de documents français et étrangers

Une *Fiche pratique n° 1* complète le référentiel régional en fournissant de nombreux exemples de pièces d'identité et des règles applicables pour l'enregistrement des identités par les structures de santé.

La version 1 a été publiée en janvier 2018. Ce document est susceptible d'être enrichi avec de nouveaux exemples issus des difficultés rencontrées signalées à la CRIV.

11.3.2 FP 2 : Foire aux questions

Les réponses aux questions posées par les professionnels sur les difficultés d'interprétation ou d'application du référentiel régional font l'objet d'une *Fiche pratique n° 2*. Les éléments de la première version de ce document, publié en janvier 2018, ont été intégrés dans le référentiel et dans la version 2 de la FP 1.

La version 1 est devenue caduque. Elle pourrait être remplacée par une nouvelle version s'il apparaît de nouveau nécessaire de répondre collectivement à des difficultés d'application ou d'interprétation de la dernière version du référentiel régional signalées à la CRIV.

11.4 Codes des pays étrangers

Pays	*Code PMSI*
AFGHANISTAN	99212
AFRIQUE DU SUD	99303
ALBANIE	99125
ALGERIE	99352
ALLEMAGNE	99109
ANDORRE	99130
ANGOLA	99395
ANTIGUA ET BARBUDA	99441
ANTILLES NEERLANDAISES	99431
ARABIE SAOUDIENNE (SAOUDITE)	99201
ARGENTINE	99415
ARMENIE	99252
AUSTRALIE	99501
AUTRICHE	99110
AZERBAIDJAN	99253
BAHAMA (ILES)	99436
BAHREIN (ILES)	99249
BANGLADESH	99246
BARBADE (ILE)	99434
BELGIQUE	99131
BELIZE	99429
BENIN	99327
BIELORUSSIE	99148
BIRMANIE (MYANMAR)	99224
BOLIVIE	99418
BOSNIE-HERZEGOVINE	99118
BOTSWANA	99347
BOUTHAN	99214

BRESIL	99416
BRUNEI (DARUSSALAM)	99225
BULGARIE	99111
BURKINA (EX HAUTE VOLTA)	99331
BURUNDI	99321
CAMBODGE	99234
CAMEROUN	99322
CANADA	99401
CAP-VERT (ILES)	99396
CENTRAFRIQUE (REPUBLIQUE DE)	99323
CHILI	99417
CHINE (REPUBLIQUE POPULAIRE DE)	99216
CHYPRE	99254
COLOMBIE	99419
COMORES	99397
CONGO (REPUBLIQUE DEMOCRATIQUE) ZAIRE	99312
CONGO (REPUBLIQUE POPULAIRE) BRAZZAVILLE	99324
COREE DU NORD	99238
COREE DU SUD	99239
COSTA-RICA	99406
COTE-D'IVOIRE	99326
CROATIE	99119
CUBA	99407
DANEMARK	99101
DJIBOUTI	99399
DOMINICAINE (REPUBLIQUE) (ST-DOMINGUE)	99408
DOMINIQUE	99438
EGYPTE	99301
EMIRATS ARABES UNIS	99247
EQUATEUR	99420
ERYTHREE	99317
ESPAGNE	99134
ESTONIE	99106
ETATS-UNIS D'AMERIQUE	99404
ETHIOPIE	99315
FALKLAND (ILES)	99427
FIDJI	99508
FINLANDE	99105
FRANCE	99100
GABON	99328
GAMBIE	99304
GEORGIE	99255
GHANA	99329
GIBRALTAR	99133
GRECE	99126
GRENADE	99435
GROENLAND	99430
GUATEMALA	99409
GUINEE	99330
GUINEE BISSAU	99392

GUINEE EQUATORIALE	99314
GUYANA	99428
HAITI	99410
HONDURAS	99411
HONGRIE	99112
ILES MARSHALL (REPUBLIQUE DES)	99515
INDE	99223
INDONESIE	99231
IRAK	99203
IRAN	99204
IRLANDE	99136
ISLANDE	99102
ISRAEL	99207
ITALIE	99127
JAMAIQUE	99426
JAPON	99217
JORDANIE	99222
KAZAKHSTAN	99256
KENYA	99332
KIRGHIZISTAN	99257
KIRIBATI	99513
KOWEIT	99240
LAOS	99241
LESOTHO	99348
LETTONIE	99107
LIBAN	99205
LIBERIA	99302
LIBYE	99316
LICHTENSTEIN	99113
LITUANIE	99108
LUXEMBOURG	99137
MACEDOINE (EX-REPUBLIQUE YOUGOSLAVE DE)	99156
MADAGASCAR	99333
MALAISIE	99227
MALAWI	99334
MALDIVES (ILES)	99229
MALI	99335
MALTE	99144
MAROC	99350
MAURICE (ILE)	99390
MAURITANIE	99336
MEXIQUE	99405
MICRONESIE (ETATS FEDERES)	99516
MOLDAVIE	99151
MONACO	99138
MONGOLIE (EXTERIEURE)	99242
MONTENEGRO	99121
MOZAMBIQUE	99393
NAMIBIE	99311
NAURU	99507

NEPAL	99215
NICARAGUA	99412
NIGER	99337
NIGERIA	99338
NORVEGE	99103
NOUVELLE-ZELANDE	99502
OMAN (SULTANAT D')	99250
OUGANDA	99339
OUZBEKISTAN	99258
PAKISTAN	99213
PALAOS (REPUBLIQUE DES)	99517
PALESTINE	99261
PANAMA	99413
PAPOUASIE-NOUVELLE-GUINEE	99510
PARAGUAY	99421
PAYS-BAS	99135
PEROU	99422
PHILIPPINES	99220
POLOGNE	99122
PORTO-RICO ET POSSESSIONS E-U.	99432
PORTUGAL	99139
QATAR	99248
ROUMANIE	99114
ROYAUME-UNI	99132
RUSSIE (FEDERATION DE)	99123
RWANDA	99340
SAHARA OCCIDENTAL	99389
SAINT CHRISTOPHE ET NIEVES (FEDERATION DE)	99442
SAINT-MARIN	99128
SAINT-VINCENT-ET-GRENADINES	99440
SAINTE-LUCIE	99439
SALOMON	99512
SALVADOR	99414
SAMOA OCC., NLLE-GUINEE OCC. OU IRIAN	99506
SAO-TOME-ET-PRINCIPE	99394
SENEGAL	99341
SERBIE	99121
SEYCHELLES (ILES)	99398
SIERRA-LEONE	99342
SINGAPOUR	99226
SLOVAQUIE	99117
SLOVENIE	99145
SOMALIE	99318
SOUDAN	99343
SRI-LANKA (CEYLAN)	99235
STE-HELENE, ASCENSION (ILES)	99306
SUEDE	99104
SUISSE	99140
SURINAM	99437
SWAZILAND	99391

SYRIE	99206
TADJIKISTAN	99259
TAIWAN (EX FORMOSE)	99236
TANZANIE	99309
TCHAD	99344
TCHEQUE (REPUBLIQUE)	99116
THAILANDE	99219
TOGO	99345
TONGA OU ILES DES AMIS	99509
TRINITE, TOBAGO	99433
TUNISIE	99351
TURKMENISTAN	99260
TURQUIE	99208
TUVALU	99511
UKRAINE	99155
URUGUAY	99423
VANUATU	99514
VATICAN (CITE DU)	99129
VENEZUELA	99424
VIET-NAM	99243
YEMEN	99251
ZAMBIE	99346
ZIMBABWE (EX RHODESIE)	99310
Inconnu	99999