REFERENTIEL
DE BONNES PRATIQUES EN MATIERE D'IDENTITOVIGILANCE EN REGION BRETAGNE

Mars 2019

Agence Régionale de Santé
Bretagne

Liste des contributeurs

A la version initiale

Ce travail réalisé par le Comité Régional d'Identitovigilance de Bretagne, s'est appuyé sur le référentiel de bonne pratique en matière d'identitovigilance communiqué par l'ARS Nouvelle-Aquitaine.

- **Membres du Comité Régional d'Identitovigilance de Bretagne (CRIB)**

Marina Bouget, Ingénieur gestion des risques, Structure Régionale d'Appui à la qualité des soins et à la sécurité des patients - CAPPS Bretagne
Céline Brillant, Responsable Facturation Territoriale et Organisation interne - Centre Hospitalier de Douarnenez et Centre Hospitalier Cornouaille Quimper
Olivier Caveau, Réfèrent identitovigilance, service d'information médicale, Hôpital d'Instruction des Armées Clermont Tonnerre, Brest
Veronique Chesnais, Ingénieur qualité gestion des risques, Structure Régionale d'Appui à la qualité des soins et à la sécurité des patients - CAPPS Bretagne
Catherine Darbo, Médecin DIM - pilote de la CIV, GHT Armor, Centre Hospitalier Guingamp
Laurence Delugin, Responsable du pôle immuno-hématologie du LBM, Etablissement Français du Sang
Marie-Josée Demay, Directrice adjointe, Centre Hospitalier Centre Bretagne, Pontivy
Yann Desreac, Responsable développement et intégration, Groupe Vivalto
Emmanuel Dudognon, Directeur adjoint des finances, Centre Hospitalier régionale Universitaire, Brest
Clément Dumortier, Responsable de l'activité immunohématologique/délivrance du site, Etablissement Français du Sang
Ingrid Felten-Vinot, Chef projet, pôle Régional de cancérologie Bretagne
Magali Fromentin, Responsable Informatique et Système d'Information, Centre Armoricain radiothérapie imagerie médicale oncologie, Plérin
Virginie Gall, Directrice adjointe des finances, Centre Hospitalier Universitaire, Rennes
Arthur Guedes, Commissaire, Hôpital d'Instruction des Armées Clermont Tonnerre, Brest
Eric Henry, Médecin Généraliste, URPS Médecins libéraux
Elodie Jamet, Ingénieur qualité et RSSI, Centre Hospitalier Centre Bretagne, Pontivy
Gilles Larroche, Chef de projet, Groupement de Coopération Sanitaire e-Santé Bretagne
Erwan Le Boulanger, Cadre Bureau des Entrées, Centre Hospitalier Universitaire, Rennes
Florence Luneau, Responsable qualité, 3C OncArmor
Laure Mahé, Chef de projet, Groupement de Coopération Sanitaire e-Santé Bretagne
Sylvie Metayer, Directrice de l'association « Appui aux professionnels de santé », Saint-Avé
Laëtitia Meudal, Responsable GAP, Centre Hospitalier de Paimpol
Sylvie Müller, Medecin correspondantes identitovigilance, Centre Hospitalier, Lorient
Beatrice Nicolas, Directrice adjointe - Direction des usagers, des services aux Patients et des Partenariats innovants, Centre Hospitalier Bretagne Atlantique, Vannes
Jean-Pierre Nicolas, Chef de projet identitovigilance, Agence Régionale de la Santé, Bretagne
Donavine Nimubona, Médecin coordinateur de réseau, Oncobretagne
Dominique Padellec, Cadre référent Identitovigilance, Centre Hospitalier Bretagne Sud, Lorient
Gérald Parolin, Psychiatre, Etablissement Public de Santé Mentale Jean Martin Charcot, Caudan
Caroline Pattier, Responsable Qualité Gestionnaire des Risques, Hospitalité Saint-Thomas de Villeneuve
Celine Perez, Attachée d'Administration à la Direction des Relations et Droits des Usagers, Centre Hospitalier de Cornouaille, Quimper
Christian Philipot, Responsable d'applications, Centre Hospitalier régionale Universitaire, Brest
Yann Prigent, Médecin Généraliste, URPS Médecins libéraux
Rozenn Rebour, TSH DIM archives médicales, Centre Hospitalier régionale Universitaire, Brest
Gwendal Rolland, Directeur, Association Pondi CLIC, Pontivy

Florence Roussel, Directrice adjointe Clientèle et projets - Responsable CIV, Centre Hospitalier, Saint-Malo

- **Participants du groupe de travail « Elaboration du référentiel de Bonnes pratiques en matière d'identitovigilance »**

Clément Dumortier, Responsable de l'activité immunohématologique/délivrance du site, Etablissement Français du Sang
Olivier Caveau, Réfèrent identitovigilance, service d'information médicale, Hôpital d'Instruction des Armées Clermont Tonnerre, Brest
Veronique Chesnais, Ingénieur qualité gestion des risques, Structure Régionale d'Appui à la qualité des soins et à la sécurité des patients - CAPPS Bretagne
Yann Desreac, Responsable développement et intégration, Groupe Vivalto
Elodie Jamet, Ingénieur qualité et RSSI, Centre Hospitalier Centre Bretagne, Pontivy
Gilles Larroche, Chef de projet, Groupement de Coopération Sanitaire e-Santé Bretagne
Erwan Le Boulanger, Cadre Bureau des Entrées, Centre Hospitalier Universitaire, Rennes
Florence Luneau, Responsable qualité, 3C OncArmor
Laure Mahé, Chef de projet, Groupement de Coopération Sanitaire e-Santé Bretagne
Jean-Pierre Nicolas, Chef de projet identitovigilance, Agence Régionale de la Santé, Bretagne
Caroline Pattier, Responsable Qualité Gestionnaire des Risques, Hospitalité Saint-Thomas de Villeneuve
Gwendal Rolland, Directeur, Association Pondi CLIC, Pontivy

SOMMAIRE

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 dispositifs de coordination assurant l'optimisation des parcours de santé des usagers. Le Programme Régional Santé de la région Bretagne 2018-2022 a bien identifié l'enjeu décisif de cette qualité de l'identification de l'usager pour la mise en place de services numériques performants et sécurisés.

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, personnels administratifs et usagers) 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 et de la prise en charge.

La consolidation1 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 diffusées à 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, Etablissement Français du Sang, 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» pour identifier les professionnels, établissements, services et organismes intervenant dans la prise en charge sanitaire, médico-sociale ou sociale ;
- « usagers » au sens des personnes accueillies par ces structures : utilisateurs du système de santé ou personnes accompagnantes (ayant-droit, personne de confiance…).

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) Bretagne pour assurer la bonne identification des usagers à toutes les étapes de leur prise en charge sur le territoire, a pour objectif:

- d'améliorer la qualité et la sécurité des prises en charge dans le cadre de la continuité

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

des soins et du partage d'informations entre professionnels intervenant dans un même parcours de santé ;

- de réduire le risque d'erreurs d'identification des personnes prises en charge ;
- de favoriser le respect des bonnes pratiques d'identification des usagers par les professionnels ;
- de garantir la confiance dans la qualité des informations échangées entre les systèmes d'information et professionnels de santé ;

Le présent référentiel de bonnes pratiques identifie un corpus de règles en matière d'identification de l'usager applicable au sein des structures sanitaires, médico-sociales et sociales, ou par tous professionnels en charge de l'identification d'un usager.

L'application de ce référentiel est un préalable :

- au développement de l'interopérabilité des systèmes d'information de santé ;
- au rapprochement d'identité entre structures différentes
- au 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 en structure: hospitalisation, consultation, visite à domicile, télémédecine…
- à tous les modes d'exercice : salarié, libéral en établissements publics ou privés
- à toutes les étapes du parcours de santé et de soins de l'usager

Les acteurs concernés sont :

- l'usager, acteur de sa sécurité ;
- 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 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 médecins, pharmaciens, dentistes, sages-femmes;
- les paramédicaux (infirmiers, aides-soignants, personnels de rééducation…) ;
- les secrétaires médicales et assistantes médico-administratives ;
- les ambulanciers et brancardiers ;
- le personnel des services médicotechniques (laboratoire, imagerie, pharmacie à usage intérieur…) ;
- les travailleurs sociaux ;
- Les psychologues
- le personnel d'accompagnement intervenant au sein des établissements et services

médico- sociaux comme ceux intervenant sur le parcours de santé (éducateurs, moniteurs d'ateliers, etc.) ;

- les intervenants de sociétés tierces réalisant des prises de rendez-vous par téléphone ;
- les industriels développant des solutions informatiques
- les agents de services mortuaires …

Il est à noter que ce référentiel de bonnes pratiques sera mis à disposition des structures sociales et sera amendé ultérieurement en fonction de leurs besoins.

2.3 Gouvernance régionale de l'identitovigilance

2.3.1 Instance de validation ARS Bretagne

Une instance de validation dédiée au projet régional « Gestion de l'identité de l'usager » a été constituée au sein de l'ARS Bretagne. Elle réunit les responsables de la Direction de la Santé Publique (DSP) et de la Direction des Coopérations Territoriales et des Performances (DCTP).

Cette instance 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 régionale, validation des voies et moyens à mettre en place, évaluation des résultats…

Elle se réunit plusieurs fois par an, en fonction des besoins, soit de façon autonome, soit sur sollicitation des référents métiers ARS ou du CRIB (Comité Régional d'Identitovigilance de Bretagne, cf 2.3.2).

2.3.2 Comité Régional d'Identitovigilance de Bretagne (CRIB)

Le Comité Régional d'Identitovigilance de Bretagne (CRIB) 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 et sociaux, de professionnels libéraux, de l'Etablissement Français du Sang, de dispositifs de coordination, de l'hôpital militaire (HIA) et des centres médicaux des armées (CMA), de l'ARS Bretagne, de la Structure Régionale d'Appui (SRA) CAPPS Bretagne et du GCS e-santé Bretagne… Le nombre et la qualité des professionnels impliqués est susceptible d'évoluer en fonction des besoins.

Cette instance a été constituée afin de proposer à l'ARS Bretagne les principales orientations de la politique régionale d'identification de l'usager. A cette fin, quatre objectifs lui sont particulièrement assignés :

- Définir les règles d'identification de l'usager en Bretagne avec pour livrable un référentiel de bonnes pratiques.
- Identifier les leviers d'une bonne appropriation de ces règles par les acteurs en région (formations, supports de communication…)
- Favoriser la convergence des politiques locales d'identitovigilance (identifier les leviers de cette convergence, élaborer une charte de rapprochement des identités entre structures, participer à la réflexion sur les outils du rapprochement)
- Accompagner au long cours les acteurs de l'identitovigilance sur les problématiques d'ordre technique et juridique

Elle se réunit plusieurs fois dans l'année, en fonction des besoins ou sur sollicitation de l'ARS

Bretagne. Pour mener à bien ses missions, ce comité peut constituer des groupes de travail ou de réflexion thématiques ayant leur propre calendrier de réunion.

Les travaux produits font l'objet de présentations régulières au sein du Réseau Régional de Vigilance et d'Appui (RREVA).

2.3.3 Cellule Opérationnelle Régionale d'Identitovigilance de Bretagne (CORIB)

Une réflexion est actuellement menée au sein de l'ARS Bretagne sur la constitution d'une CORIB. La composition de cette instance ainsi que ces missions seront détaillées dans une version ultérieure du référentiel de bonnes pratiques.

Cette cellule sera particulièrement chargée de favoriser et d'accompagner le déploiement du référentiel, de contribuer à faire adhérer les structures et les industriels, de piloter la gestion des risques lors du rapprochement des identités.

2.4 Gestion locale de l'identitovigilance

Pour la bonne mise en œuvre de la politique d'identitovigilance, chaque structure veillera à mettre en place une organisation, adaptée(s) à sa taille et à son activité.

Des instances pourront être mutualisées entre différents établissements/services utilisateurs du même outil de gestion de l'usager.

A minima, il est demandé à chaque structure et organisation dans les champs médico-social et ambulatoire de :

- définir une politique d'identitovigilance et une charte d'identification des usagers s'inscrivant dans le présent référentiel,
- de désigner un référent local d'identitovigilance qui sera en charge de toutes les questions relatives aux bonnes pratiques d'identification des usagers depuis leur accueil jusqu'à l'archivage de leurs dossiers
- de signaler les dysfonctionnements liés à l'identitovigilance sur le portail national des signalements lors qu'il s'agit d'évènements indésirables graves associés aux soins (y compris ceux liés au système d'information).
- De mettre en place des actions préventives et correctives des dysfonctionnements en lien avec l'identitovigilance

En ce qui concerne le champ sanitaire, il conviendra de 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 structure (ou le groupe de structure) définit :

- 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 sur le portail national des signalements lors qu'il s'agit d'évènements indésirables graves associés aux soins (y compris ceux liés au système d'information;
- 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.

A cette fin, elle peut s'appuyer sur un comité d'identitovigilance, une autorité de gestion des identités ou une autre instance stratégique existante en son sein.

2.4.2 Niveau opérationnel

Le niveau opérationnel a 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 (usager 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 collisions ;
- 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.

A cette fin, une Cellule d'IdentitoVigilance peut être mise en place.

2.4.3 Référent d'identitovigilance

Un référent local d'identitovigilance, désigné par la structure, est l'interlocuteur privilégié pour toutes les questions relatives aux bonnes pratiques d'identification des usagers depuis leurs accueils jusqu'à l'archivage de leurs dossiers.

Il peut être amené à organiser et animer les réunions de la CIV, à participer aux travaux du niveau stratégique, à délivrer l'information et les formations relatives à l'identitovigilance.

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, 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 divers services de la structure pour constituer un relais au plus près du terrain (informations montantes et descendantes) et participer au déploiement local des actions d'amélioration.

2.5 Charte d'identitovigilance

Il est recommandé que chaque structure décline la politique institutionnelle d'identification de

l'usager au sein d'une charte d'identitovigilance, adaptée à sa taille 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 administratives et médicales en évitant les doublons et collisions ;
- harmoniser et rendre compatibles les procédures locales existantes, préalables indispensables aux rapprochements d'identité inter-structures 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 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. 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.

3 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.

3.1 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 pièce 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) ;
- la date de naissance ;
- le sexe ;

N.B : Conformément au décret n° 2017-412 du 27 mars 2017, l'Identifiant National de Santé (INS) pourra entrer dans cette catégorie.

3.2 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 ;
- le lieu de naissance : département, commune et/ou code postal pour un ressortissant français, code PMSI ou ISO du pays pour un étranger).

3.3 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:

- l'adresse courriel de contact ;
- l'adresse de résidence de l'usager ou de l'assuré ;
- les autres professionnels de santé impliqués dans la prise en charge ;
- l'INS-C (si calculé)
- le médecin traitant ;
- le nom des personnes en relation (parent, enfant, conjoint, personne de confiance…) ;
- les numéros de téléphone ;
- la photographie de l'usager
- la profession ;
- …

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.

4 VALIDITE DE L'IDENTITE RECUEILLIE

4.1 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 « **validée »** que lorsqu'elle est relevée à partir d'un document d'identité officiel et en cours de validité comportant les traits stricts :

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

Tout autre document non listé ci-dessus, ne peut être considéré comme validant, par conséquent l'identité doit être considérée comme provisoire (livret de famille, permis de conduire, extrait d'acte de naissance, document de demandeur d'asile avec photo, document de justice…)

Il est rappelé que les données enregistrées sur la carte Vitale ne sont actuellement pas suffisamment fiables pour valider l'identité d'un usager.

En cas de suspicion d'usurpation d'identité, il est demandé aux structures de se référer aux procédures locales en vigueur et d'assurer la bonne transmission de l'information à l'ensemble des personnes (ou structures) prenant également en charge l'usager.

4.2 Discordances entre documents d'identité

S'il existe des différences entre documents de même 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, la structure est invitée 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 « validée ».**

4.3 Cas particulier des identités recueillies par les applications régionales

Les procédures d'identification suivies par les applications régionales doivent à minima assurer la complétion des traits stricts définis en section 3.1.

L'identité produite par ce type d'application restera provisoire jusqu'à présentation d'un document officiel d'identité à une personne habilitée à créer ou valider l'identité d'un usager, ou application des deux modes de validation complémentaires décrits en section 4.4.3.

4.4 Gestion de l'identité numérique fournie par l'usager à distance

Le ministère de la santé, dans sa **stratégie nationale e-santé 2020** réaffirme son souhait de renforcer et simplifier l'accès aux soins à l'usager. La qualité des séjours hospitaliers peut être optimisée via des « portails patients » de prises de rendez-vous et/ou de préadmission en ligne. Ces applications numériques doivent permettre une meilleure transmission des informations entre les différents partenaires intervenants dans la prise en charge de l'usager quel que soit leur mode d'exercice (salarié, libéral).

4.4.1 Identités produites par des plateformes de prise de rendez-vous en ligne

Les systèmes de prise de rendez-vous en ligne permettent à l'usager de trouver un professionnel de santé, près de chez lui et de prendre rendez-vous à tout moment de la journée.

Les procédures d'identification suivies par ces plateformes doivent à minima assurer la complétion des traits stricts définis en section 3.1. Il est conseillé de mettre en place un circuit de validation de l'identité de l'usager en adéquation avec les niveaux de confiance des documents d'identité détaillés au point 4.1. En fonction de l'organisation définie en interne, cette validation d'identité sera faite par une personne habilitée aux bureaux des admissions ou par le professionnel en consultation ou son secrétariat.
Il est recommandé d'expliciter la démarche à suivre dans la procédure de validation d'identité en vigueur au sein de la structure. Des actions de sensibilisation peuvent être mises en place pour accompagner les différents acteurs de l'identitovigilance dans le déploiement de ce type d'application numérique.

En complément des informations pratiques précisées sur la plateforme (emplacement, honoraires…), la structure pourra repréciser les documents administratifs à apporter pour la consultation (section 4.1).

4.4.2 Identités produites par des plateformes de préadmission en ligne

En cas d'hospitalisation programmée et/ou de consultation, la structure de soins peut mettre à disposition des usagers, des plateformes de préadmission en ligne. La constitution au préalable du dossier permettra à l'usager le jour du rendez-vous de gagner un temps conséquent aux lieux recueillant l'identité (ex : secrétariat de consultations…) et d'éviter tout oubli de pièces obligatoires à la constitution de son dossier.

Il est conseillé pour la structure mettant à disposition ce service, d'accompagner au mieux l'usager dans la complétion de son dossier de préadmission en respectant à minima la complétion des traits stricts.

Ce portail de préadmission est l'opportunité pour la structure de repréciser les documents administratifs à apporter lors de l'admission de l'usager en mettant l'accent sur les documents d'identité officiels à jour et en cours de validité (section 4.1).

4.4.3 Modes de validation des identités numériques

A titre d'exemple, les trois modes de validation suivants peuvent être implémentés localement :

- un document d'identité validant a été fourni et vérifié par à une personne habilitée
- un système d'authentification type FranceConnect a été intégré au service en ligne
- un document officiel a été vérifié par une solution de vérification automatisée d'identité.

4.5 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 nom. En cas d'adoption simple, le nom du ou des adoptants peut s'ajouter ou remplacer le nom de l'adopté (cf article 355 à 359 du code civil)
- Dans le cas d'un changement de nom de famille (naissance), du prénom, du lieu ou de la date de naissance, une attestation de concordance d'identité doit être demandée au consulat ou aux autorités du pays d'origine de l'intéressé.

- 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 (cf. article L.213-1 du Code du patrimoine issu de l'article 17 de la loi n° 2008-696 du 15 juillet 2008 relative aux archives).
- 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 le référent identitovigilance. Il convient toutefois d'être attentif sur les modalités pratiques de cette opération (insertion dans le dossier papier ou informatique) et la durée de conservation de ce document. La structure 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.

5 REGLES POUR LA CREATION D'UNE IDENTITE

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

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'incapacité 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 (S2RI).

Les règles à appliquer en Bretagne seront revues dans la cadre de la publication du futur arrêté portant sur l'approbation du référentiel « Identifiant National de Santé ». Une procédure annexe sera élaborée à cet effet.

5.1 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** ». Cette règle est applicable dans le cas de dates de naissance en décile lunaire.
- 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*).

[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).

- 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.

5.2 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 (naissance) 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 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.

6 REGLES D'APPLICATION EN MATIERE D'IDENTITOVIGILANCE

La qualité des données qui composent la base de données des usagers est primordiale. Les structures 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/VIP …

6.1 Référentiel d'identité

Au sein d'une structure, 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 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. Cette opération est réalisée après contrôle immédiat ou secondaire des documents d'identité (cf.4).

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 la première lettre du nom de famille (naissance) et du prénom, 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.

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 entre 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) ou au référent local d'identitovigilance par tout professionnel constatant l'erreur, 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.7.3.1), 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 la structure. Elle est diffusée au personnel et aux nouveaux arrivants.

6.5.2 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.

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

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.

6.5.3 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 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 ;
- Signalement d'erreur d'identité ;
- 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/VIP/confidentiel ;
- 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. Elle est décrite dans une procédure spécifique.

Elle ne peut être réalisée qu'au vu d'un document d'identité officiel (cf. 4.1), 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 autorisée que pour des personnels spécialement habilités, sous le contrôle de la structure. 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 soit 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.

7.2 Identification des homonymes

La notion d'homonymie est définie entre deux identités (à minima) comme :

- la correspondance exacte de l'ensemble des traits stricts (décrits au 3.1) : homonyme parfait
- la correspondance exacte de plusieurs traits stricts avec au moins un homophone (ex : DUPOND et DUPONT) : homonyme imparfait

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…).

Attention : lors de l'arrivée d'un usager 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.

7.3 Identification secondaire

7.3.1 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.

7.3.2 Dispositifs d'identification physique

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

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, usager 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).

7.3.3 Identification des documents du dossier de l'usager

Les structures 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 l'usager 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 et prendre en compte tous les aspects de l'identitovigilance.

Elle doit aussi concerner les intervenants externes : ambulanciers, brancardiers, 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 (article L162-21 du code de la sécurité sociale, applicable pour les établissements de santé).

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

Bon à savoir :

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.

8.3 Respect des droits des usagers

Les structures respectent le droit des usagers s'appliquant à leur domaine d'activités, et notamment :

- d'être informé en cas de traitement des données les concernant ;
- d'avoir accès aux données personnelles les concernant ;
- de demander la rectification des données erronées ou périmées ;
- d'avoir la garantie de la confidentialité des données les concernant…

9 INDICATEURS QUALITE

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

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 validée/provisoire ;
- Nombre d'usurpations d'identités détectées ;
- Taux de fiches de signalement d'événements indésirables (FSEI) relatives à l'identification des usagers ;
- Indicateurs qualité et de la sécurité des soins (IQSS) 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 usagers différents, 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 s'agit à réattribuer à chaque usager concerné par une collision 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 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 sont assurés 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 disjoints. Le fait de ne pas disposer de l'ensemble des informations 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 (cf. 7.2) est définie entre deux identités (à minima) comme :

- la correspondance exacte de l'ensemble des traits stricts (décrits au 3.1) : homonyme parfait
- la correspondance exacte de plusieurs traits stricts avec au moins un homophone (ex : DUPOND et DUPONT) : homonyme imparfait

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)

Le numéro d'inscription au répertoire des personnes physiques (NIRPP ou 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).

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 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 ».

Pour les personnes nées à l'étranger, il est attribué un NIA, numéro identifiant d'attente attribué par la CNAV (Caisse Nationale d'Assurance Vieillesse) 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).

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.

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 et ne peut être enregistré que dans les systèmes d'information qui dispose d'un champ spécifique.

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 au moins 2 structures, 2 applications d'une même structure…

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.