Groupe de travail régional d'identitovigilance
de Nouvelle-Aquitaine

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

Version 1 du 26 juin 2017

Liste des contributeurs

- Mme Marie-Pierre BAUDON, chargée de mission système d'information, Agence régionale de santé Nouvelle-Aquitaine
- M Yves BEAUCHAMP, manager à l'Agence nationale d'appui à la performance
- Dr Yann BLANCHARD, Département d'information médicale, Centre hospitalier de la Côte Basque
- Mme Tiphaine BONDY, responsable de la cellule d'identitovigilance, Etablissement français du sang Aquitaine Limousin
- 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, Centre hospitalier universitaire de Bordeaux
- Mme Delphine FLESCQ, chargée de mission au pôle qualité sécurité des soins, Agence régionale de santé Nouvelle-Aquitaine
- 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 Centre hospitalier universitaire de Bordeaux
- Dr Isabelle JAMET, responsable du pôle études, statistiques et évaluation, Agence régionale de santé Nouvelle-Aquitaine
- Dr Nadia KHALDI, responsable des vigilances, Etablissement français du sang Aquitaine Limousin
- 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 Philippe MURAT, pharmacien général de santé publique, référent biologie, Agence régionale de santé Nouvelle-Aquitaine
- Dr François NASSIRI, Santé-Landes
- Mme Christelle NOZIERE, chef de projet EPSILIM, Limoges
- Mme Dany OULEY, ingénieur qualité, Cellule d'identitovigilance et de rapprochement du Centre hospitalier universitaire de Bordeaux
- Dr Jean-Luc QUENON, codirecteur du Centre de coordination de l'évaluation clinique et de la qualité en Nouvelle-Aquitaine (CCECCQA)
- Dr Florence PERRET, Département d'information médicale, Maison de santé Marie Galène
- Dr Catherine RAUTURIER, directeur médical ADAPEI 33
- Mme Sylvie RIBET, responsable de l'identitovigilance, Groupe Bordeaux Nord Aquitaine
- Dr Bernard TABUTEAU, médecin conseiller au pôle qualité et sécurité des soins, Agence régionale de santé Nouvelle-Aquitaine.

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 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 (soignants 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 annexe (cf. « 7.2 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 Niveau stratégique

L'ARS pilote un comité régional stratégique chargé de définir la politique et la stratégie à mettre en œuvre dans la région pour améliorer les pratiques dans le domaine de l'identitovigilance et sensibiliser les différentes parties prenantes.

2.3.2 Niveau opérationnel

Une cellule opérationnelle d'identitovigilance régionale (CIVR) est chargée de la gestion des risques dans ce domaine : conduite du plan régional d'actions, traitement des anomalies au niveau du serveur régional de rapprochement d'identité, suivi des indicateurs…

2.4 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.

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 (accouchement sous X…).

Des critères doivent permettre de distinguer les identités réelles et vérifiées 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 et 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.

2.5 Modèle régional d'identification de l'usager

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

2.5.1 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 le plus récent possible 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 ;
- le lieu de naissance (département et commune pour un ressortissant français, pays pour un étranger).

2.5.2 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 (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.

2.5.3 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'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 ;
- la pièce d'identité présentée…

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 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…

3 GESTION DES RISQUES 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...

3.1 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.

3.2 Recueil de l'identité

Dans les structures de santé, la saisie de l'identité de l'usager dans le SI est réalisée sous la responsabilité de professionnels habilités en interne à le faire (cf.3.8.2) : bureau des entrées, urgences, secrétariat médical…

3.3 Validation de l'identité

L'identité ne doit être validée que par un personnel habilité à le faire (cf. 3.8.2), après contrôle immédiat ou secondaire 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 :

- elle est « **certifiée »** lorsqu'elle est relevée à partir d'une pièce d'identité officielle comportant les traits stricts et une photo récente ;
- elle est « **qualifiée** » lorsqu'elle se base sur d'autres documents officiels ;
- elle est « **provisoire** » dans tous les autres cas.

Il est recommandé de disposer par ailleurs d'une qualification « **douteux** » pour identifier les cas où l'identité recueillie est suspecte : risque 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.

Les documents d'identité officiels permettant de **certifier** une identité, y compris pour les étrangers, sont les suivants :

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

Les autres documents pouvant être pris en compte pour **qualifier** une identité sont :

- le livret de famille, pour les mineurs ne possédant pas de pièce 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.

Il peut être proposé d'associer plusieurs documents afin d'améliorer le niveau de confiance à accorder. En cas de discordance entre plusieurs documents produits, c'est celui ayant le plus fort niveau de confiance qui doit être pris en compte. Il convient alors d'inviter l'usager à faire corriger les données erronées par l'organisme compétent.

L'identité ne peut être que « provisoire » tant qu'un document qualifiant 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.

Remarque : les identités provisoires n'ont pas vocation à être transmises au serveur régional de rapprochement d'identité.

3.4 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 par la saisie de critères de recherche supplémentaires sur d'autres traits stricts.

3.5 Règles de saisie pour la création d'une identité

Compte-tenu de l'instruction DGOS/MSIOS du 7 juin 2013 relative à l'identification des patients, il est demandé d'appliquer des règles strictes dans toutes les structures de santé de la région.

Pour autoriser les rapprochements entre structures, il faut au minimum :
- recopier de façon la plus fidèle possible les traits stricts des documents d'identité présentés ;
- ne pas utiliser des lettres majuscules accentuées ;
- interdire toute abréviation (ex : ST pour SAINT, J PIERRE pour JEAN-PIERRE).

Ces caractères étant destinés à être remplacés par des espaces lors des opérations de rapprochement, il est possible de recopier les caractères de ponctuation (apostrophes, tirets, parenthèses) tels qu'utilisés dans les documents officiels.

3.5.1 Règles particulières concernant les traits stricts

- En l'absence de prénom, il faut saisir les informations telles qu'elles apparaissent sur la pièce d'identité (exemples : XX, SP, SANS PRENOM) ;
- Si le jour de la naissance est inconnu, on enregistre par défaut « 01 », soit le premier jour du mois. Si le mois n'est pas connu, on enregistre par défaut le mois de janvier (« 01 »). 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]. Si l'année n'est pas connue précisément, on enregistre par défaut la décennie. 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 la pièce

[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).

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).

3.5.2 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 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. 3.6).
- Pour les structures de santé qui disposent d'un logiciel obligeant à saisir un nom d'usage, il faut recopier le nom de famille (naissance) dans ce champ pour les usagers qui n'en disposent pas.

3.5.3 Règles formalisées dans des procédures spécifiques

Il est particulièrement important de formaliser dans des procédures opérationnelles les consignes à appliquer lorsque l'identification formelle du patient n'est pas garantie :
- enregistrement d'un usager incapable de donner ou justifier son identité ;
- homonymie ;
- suspicion d'usurpation d'identité ;
- usager souhaitant garder son anonymat ;
- identification de victimes lors d'afflux massif ;
- identification de personnes étrangères disposant de cartes d'identité ou passeports de leur pays d'origine, etc.

3.6 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 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 soient bien distingués :
- 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 :
Prénom d'usage	Prénom usage :	Pr.Us :

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

Toute anomalie doit être signalée sans délai à la (aux) cellule(s) d'identitovigilance concernée(s) pour mise en œuvre sans délai 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, doit être mise en œuvre afin d'informer la (ou les) structure(s) concernée(s).

3.7 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.

3.7.1 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 régional d'identitovigilance (CRIV).

3.7.2 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.

3.7.3 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 d'identitovigilance régionale (CIVR) 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.

3.7.4 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.

3.8 Sécurité du système d'information

3.8.1 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.

3.8.2 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.

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

3.8.3 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.

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.

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

3.8.4 Identification des homonymes

La notion d'homonymie est définie comme la correspondance exacte entre plusieurs traits stricts (décrits au 2.5.1).

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.

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.

3.8.5 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.

3.8.6 Référents logiciels

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

4 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 provisoire de l'usager en situation d'urgence ;
- Identification des victimes lors de situation sanitaire exceptionnelle ;
- Contrôle qualité des bases d'identités ;
- Recherche d'un usager dans la base ;
- Correction et rapprochement d'identités (et/ou fusion) ;
- Admission d'un usager à l'identité non connue ;
- Gestion d'une suspicion d'usurpation d'identité ;
- Admission d'un usager souhaitant garder l'anonymat ;
- Identification secondaire d'un usager avant tout acte de soin ;

- Gestion de l'identification primaire et secondaire en cas de panne du système d'information ;
- Utilisation d'un bracelet d'identification ;
- Gestion des identités dans les logiciels non ou incomplètement interfacés.

4.1 Modification et rapprochement d'identité

4.1.1 Modification d'identité

La modification d'identité n'est autorisée que pour des personnels habilités de la structure de santé (cf. 3.8.2). Elle est décrite dans une procédure spécifique.

Elle ne peut être réalisée qu'au vu d'une pièce d'identité officielle 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.

Après modification d'identité, 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 la nouvelle identité.

4.1.2 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. 3.8.3), 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 »).

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.

4.1.3 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. 3.8.6).

4.2 Identification secondaire

4.2.1 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 est à définir dans la charte d'identitovigilance (cf. 2.4) 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.

4.2.2 Dispositifs d'identification physique

La pose d'un bracelet d'identification participe à la bonne identification des personnes, sous réserve d'une acceptation de l'usager. Il est fondamental qu'il soit mis en œuvre dans les structures qui accueillent des usagers avec lesquels la communication est difficile : non francophone, patient incapable de parler, confus, inconscient, dément…

Elle doit faire l'objet d'une procédure qui décrit :

- l'information de l'usager, de sa famille ou de sa personne de confiance ;
- le recueil de son accord ;
- les modalités de préparation, de pose et dépose du bracelet ;

- la conduite à tenir en cas de refus ou de nécessité de dépose du bracelet en cours de séjour, qu'elle qu'en soit la raison ;
- les modalités pratiques d'utilisation…

Il ne doit pas y avoir de transcription manuelle de l'identité de l'usager sur le bracelet (source d'erreur) mais il faut privilégier les bracelets comportant une identité imprimée à partir des données informatisées (cf. 3.6).

Selon le contexte, d'autres dispositifs peuvent être utilisés dans certains services, comme la photo d'identité intégrée au dossier patient.

4.2.3 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.

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

5 FORMATION ET SENSIBILISATION A L'IDENTITOVIGILANCE

5.1 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…

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

5.2 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.

5.3 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 (pièce d'identité officielle notamment).

6 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…

7 ANNEXES

7.1 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 non 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.

7.2 Glossaire

7.2.1 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.

7.2.2 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.

7.2.3 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.

7.2.4 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.

7.2.5 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.

7.2.6 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.

7.2.7 Fusion

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

7.2.8 Homonymie

La notion d'homonymie est définie comme la correspondance exacte entre plusieurs traits stricts (cf. 3.8.4).

7.2.9 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)…

7.2.10 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.

7.2.11 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…).

7.2.12 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.

7.2.13 Interopérabilité de systèmes informatiques

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

7.2.14 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.

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

7.2.15 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.

7.2.16 Nom d'usage

Il correspond au nom de famille d'un tiers (« 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) ».

7.2.17 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 peut être composé, qui sert de prénom de naissance ; il est celui qui apparaît avant la virgule sur la carte d'identité. Le tiret est utilisé pour assurer le lien entre les 2 éléments d'un prénom composé ; il est remplacé par un espace pour certains prénoms d'origine étrangère notamment pour les vocables Thi, Van, Ben, Ould…

Remarque : 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.

7.2.18 Prénom d'usage

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

7.2.19 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 Halliday »

7.2.20 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…

7.2.21 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 »

7.2.22 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.

7.2.23 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.