MODELE DE CHARTE IDENTITOVIGILANCE

REGION OCCITANIE

Version 2022

01/08/2022

Table des matières

01 Introduction

01.1 – Définition et objectifs

Une charte est un document officiel destiné à établir des objectifs, des valeurs, des principes ou des règles partagées.

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.

Ce document doit y décrire les engagements pris par la structure (comprenant les professionnels qui lui sont rattachés) et les moyens mis en œuvre en termes de processus, procédures, ressources humaines et moyens techniques, tout en restant conforme à la charte du patient hospitalisé (cf. Annexe § 08.1).

En effet, la bonne identification d'un usager est un facteur clé de la sécurité de son parcours de santé. Elle constitue le premier acte d'un processus qui se prolonge tout au long de sa prise en charge par les différents professionnels de santé impliqués, quels que soient la spécialité, le secteur d'activité et les modalités de prise en charge.

Une attention particulière est à porter sur le fait que cette vigilance doit devenir opposable, au même titre que les autres vigilances réglementaires.

Le présent document propose un modèle à adapter en fonction des spécificités locales de la structure concernée, tout en conservant la trame générale dans son ensemble (plan).

01.2 – Engagements de la structure

Chaque structure de santé doit disposer d'un référentiel unique d'identité qui garantit la cohérence des données d'identités des patients tout au long de leur prise en charge, à toutes les étapes de leur parcours.

La charte d'identitovigilance a pour objet de formaliser les règles à respecter dans la perspective de :

- Recueillir l'identité exacte des patients au sein de chaque domaine d'identification recensé dans la structure
- Sécuriser les informations médicales en évitant les doublons et collisions (une bonne identification sécurise le parcours du patient)

- 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.

En accord avec les nouveaux textes publiés, le recueil et le traitement de ces données d'identité se doivent d'être conformes au Référentiel National d'Identito Vigilance (RNIV) et de ses annexes (cf. Annexe § 08.1).

La charte d'identitovigilance construite au niveau local devra s'appuyer sur des procédures liées aux types de prises en charge réalisées et les mesures de sécurité mises en place. Ces procédures seront disponibles dans un espace de type « Gestion Electronique des Documents » (GED) et devront être jointes à la charte.

01.3 – Périmètre / Acteurs concernés

Sont concernés par cette politique d'identitovigilance :

- Les professionnels de santé prenant en charge les patients,
- Les professionnels qui interviennent sur les données médico-administratives
- Les usagers (y compris les ayants-droits et les personnes de confiance), en tant qu'acteurs de la sécurité.

La constitution d'une matrice d'habilitations est nécessaire (liste fermée de personnes soumises à autorisation), et devra être exposée dans le paragraphe traitant de la gestion des risques (Chapitre 04).

01.4 – Gouvernance

Aux fins de garantir une bonne application de la politique d'identitovigilance au sein de la structure, il est nécessaire de mettre en place une ou plusieurs instances de gouvernance, tant au niveau local que territorial (cf. Annexe § 08.1).

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.

De fait, cette gouvernance de l'identitovigilance devra comprendre a minima :

- Une autorité de Gestion des Identités (AGI) qui définit la politique d'identitovigilance au sein de la structure
- Une Cellule d'Identito Vigilance (CIV) qui met en œuvre la politique d'identitovigilance
- Un Référent/Pilote Identito Vigilance qui est l'interlocuteur privilégié pour toutes les questions relatives à l'identitovigilance

A noter que pour les petites structures, l'AGI peut être associée à la CIV ou être pilotée au niveau d'un groupe/groupement.

02 Eléments d'identification

02.1 – Vocabulaire de l'identitovigilance / Terminologie

Ce glossaire permet de définir les différents termes utilisés en identitovigilance :

- Identité : ensemble des traits d'état civil caractérisant une personne.
- Identité numérique : représentation d'un individu physique dans un système d'information.
- Identifiant : code unique associé à l'identité numérique d'un individu.
- Identité INS (identité nationale de santé) : identité numérique de référence utilisée dans le secteur sanitaire, issue de l'appel au téléservice INSi de la base d'identité nationale de référence (INSEE).
- Identification : opération permettant d'établir l'identité d'un individu au regard de l'état-civil.
- Identification primaire : opération destinée à attribuer une identité numérique spécifique à un usager.
- Identification secondaire : contrôles de cohérence concernant l'identification de l'usager ou des documents qui le concernent, mis en œuvre pour s'assurer de délivrer le bon soin au bon patient.
- Identitovigilance : organisation mise en œuvre pour fiabiliser l'identification de l'usager et de ses données de santé.
- Validation de l'identité numérique : contrôle de cohérence avec l'identité officielle de la personne physique attestée par un dispositif à haut niveau de confiance.
- Récupération de l'identité INS : recherche de l'identité INS d'un usager par le téléservice INSi et enregistrement des résultats dans les traits stricts de son identité numérique, après contrôle de cohérence avec les traits de la personne prise en charge.

- Vérification de l'identité INS : contrôle de cohérence des traits de l'identité INS enregistrée ou transmise lors d'un appel au téléservice INSi, par rapport aux traits déjà présents dans le système d'information de santé ou sur une pièce d'identité de référence.
- Qualification de l'identité : action de qualifier l'identité INS après qu'elle ait été validée et récupérée.

02.2 – Domaines d'identification et de rapprochement

Le domaine d'identification (DI) est le périmètre au sein duquel chaque patient est représenté par un seul Identifiant Permanent du Patient (IPP). Chaque DI identifie le patient de façon propre avec un identifiant interne. En effet, toute structure de santé doit disposer d'un référentiel unique d'identité qui garantit la cohérence des données d'identités des patients tout au long de leur prise en charge.

Le rapprochement est l'opération qui consiste à créer un couple d'identités issues de deux DI distincts et correspondant à une même personne physique. Les deux domaines d'identification sont alors dits « domaines rapprochés ».

02.3 – Identité Nationale de Santé / NIR, NIA, NSS, matricule INS

02.31 – Identité Nationale de Santé

Cette identité numérique de référence est composée :

- Du matricule INS, associé à un *object identifier* (OID) qui précise la nature du matricule (NIR ou NIA) ;
- Des traits INS d'identité tels qu'ils sont enregistrés dans les bases nationales de référence (nom de naissance, prénom(s) de naissance, date de naissance, sexe et code INSEE du lieu de naissance).

L'identité INS peut être récupérée et/ou vérifiée par les professionnels de santé au moyen d'un téléservice dédié appelé INSi, géré par l'Assurance maladie.

02.32 – NIR, NIA, NSS, matricule INS

Les personnes nées en France et les étrangers qui y travaillent sont inscrits dans le Répertoire national d'identification des personnes physiques (RNIPP). Chaque individu recensé possède un identifiant unique dans ce registre qui est appelé NIR (numéro d'inscription au registre). L'attribution d'un NIA (numéro identifiant d'attente) est réalisée pour les personnes non nées en France avant qu'un NIR ne

soit définitivement associé aux traits d'identité de référence issus de l'état civil.

Le NIR constitue le numéro de sécurité sociale (NSS) d'une personne affiliée à un régime d'assurance maladie obligatoire. Cette affiliation lui permet le cas échéant d'« ouvrir des droits » à d'autres personnes dites « ayant droits » (ses enfants mineurs par exemple). Dans ce cas, la personne « ayant droit » peut être identifiée via son propre NIR ou via le triplet suivant : NIR de l'ouvrant droit, date de naissance de l'ayant droit et son rang de naissance. Le terme numéro de sécurité sociale est en particulier à employer lorsqu'il est fait référence à des frais de santé ou des prestations prises en charge par un organisme d'assurance maladie obligatoire.

Le NIR constitue également le matricule INS. À la différence du NSS, il est unique pour chaque individu. Le terme matricule INS est à employer lorsqu'on parle de référencement des données de santé.

02.4 - Niveau / Statut de confiance de l'identité numérique

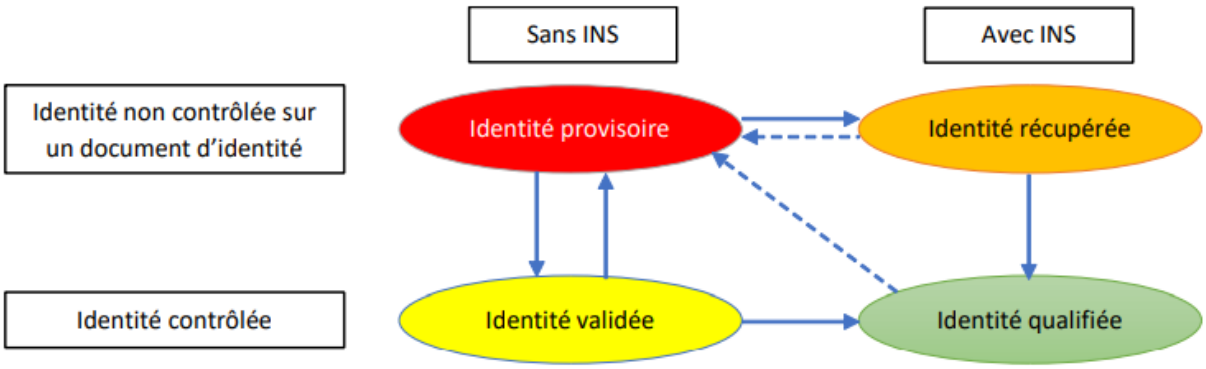
La confiance dans l'identité numérique d'un usager dans les domaines sanitaire et médico-social repose sur deux piliers majeurs :

- La validation des traits stricts lors d'un contrôle de cohérence avec l'identité de l'usager réalisé à partir d'un dispositif d'identification à haut niveau de confiance.
- La récupération ou la vérification de l'identité INS (traits stricts officiels) par appel au téléservice INSi.

En fonction de la conformité à ces deux critères cumulatifs, il est attribué un des quatre statuts de confiance à l'identité numérique (information qu'il est conseillé d'afficher sur les écrans) :

- Le statut **Identité provisoire** est attribué à toute identité numérique créée sans utilisation du téléservice INSi et sans contrôle de cohérence des traits par l'intermédiaire d'un dispositif d'identification à haut niveau de confiance
- Le statut **Identité validée** est attribué après contrôle de cohérence des traits enregistrés en identité provisoire avec ceux portés par un dispositif d'identification à haut niveau de confiance
- Le statut **Identité récupérée** correspond à l'identité INS enregistrée (ou vérifiée) après interrogation du téléservice INSi, sans contrôle de cohérence des traits par l'intermédiaire d'un dispositif d'identification à haut niveau de confiance

- Le statut **Identité qualifiée** associe la récupération de l'identité INS (ou sa vérification) à partir du téléservice INSi et le contrôle de cohérence des traits enregistrés avec ceux portés par un dispositif d'identification à haut niveau de confiance.



Seul le statut **Identité qualifiée**, le plus haut niveau de confiance d'une identité numérique, permet de référencer et transmettre les données de santé avec le matricule INS.

En cas de doute, quelle qu'en soit l'origine (manque d'informations, suspicion de fraude, etc.), le statut de l'identité doit rester « provisoire ».

03 Modèle d'identification de l'usager

03.1 – Identification primaire

L'identification primaire comporte les étapes de recherche, de création et/ou de modification de l'identité numérique attribuée en propre à un usager dans le système d'information de la structure ou du professionnel qui le prend en charge. Elle comprend l'attribution d'un statut de confiance aux données enregistrées. Cette identité numérique est constituée d'un jeu de traits qui sont propres à chaque usager. Ces traits peuvent être stricts ou complémentaires.

Les règles de recueil et saisie de l'identité sont définies en § 04.2 / § 04.5

03.1.1 - Les traits stricts

Ce sont les traits de référence qui définissent l'identité officielle d'un usager de la santé sans risque d'erreur : données stables et invariables de l'état civil, vérifiables à partir de documents d'identité officiels.

Ils comportent cinq traits minimum et obligatoires pour créer une identité (et utilisés pour un rapprochement d'identités) :

- Le nom de naissance (nom de famille) (Cf. Annexe § 08.1),
- Le premier prénom de naissance[1],
- La date de naissance[2],
- Le sexe,
- Le lieu de naissance (code INSEE de la commune de naissance pour les personnes nées en France ou du pays de naissance pour les autres[3]).

Ils doivent être complétés dès que possible par la liste des prénoms de naissance et le matricule INS, pour les usagers qui en ont un.

L'individualisation du premier prénom de naissance est nécessaire pour des raisons de compatibilité avec de nombreux logiciels de santé qui ne sont pas encore adaptés aux nouvelles règles d'identitovigilance.

La règle de définition du premier prénom peut être précisée dans une procédure interne à la structure ; en envisageant les cas, par exemple, où il n'y a pas de virgules entre les prénoms, les prénoms doubles avec ou sans tiret, etc.).

03.1.2 - Les traits complémentaires

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 patients (touristes étrangers, personnes en situation irrégulière).

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

---

[1] Champ conservé pour le moment aux fins d'assurer la compatibilité entre logiciels.
[2] 31 décembre d'une décennie compatible avec l'âge si inconnu (Cf. Annexe § 08.1)
[3] 99999 si inconnu

Enregistrés dans des champs dédiés, ils comprennent (liste non limitative) :

- Le nom et le prénom utilisés dans la vie courante
- Le code postal et/ou nom de la commune de naissance
- L'adresse postale de l'usager
- Les numéros de téléphone de l'usager ou de son tuteur
- L'adresse mail de l'usager ou de son tuteur
- La photographie
- La profession
- Le numéro de sécurité sociale de l'ouvrant droit (il concerne les différents ayants droit d'un seul assuré)
- L'identités et les coordonnées des personnes en relation (parent, enfant, conjoint, personne de confiance…)
- Le numéro de téléphone ou l'adresse mail de l'ouvrant droit
- Les coordonnées du médecin traitant
- Les autres professionnels de santé impliqués dans la prise en charge
- La nature du document d'identité présenté
- Etc.

Ces traits peuvent faire l'objet d'une définition précise et limitative au sein d'une procédure interne de la structure.

03.1.3 - Les documents validant / Dispositifs à haut niveau de confiance

Les documents d'identité officiels permettant de valider une identité de manière forte (sur présentation de ceux-ci), y compris pour les étrangers, sont les suivants :

- La carte nationale d'identité (CNI) pour les ressortissants de l'Union Européenne (UE), de la Suisse, du Liechtenstein, de la Norvège, de l'Islande, du Vatican ainsi que des Principautés de Monaco, Saint Marin et Andorre
- Le passeport
- Le titre de séjour
- L'acte ou l'extrait d'acte de naissance, pour un enfant né en France (accompagné d'un titre de haut niveau de confiance d'un parent)
- Le livret de famille, pour les mineurs ne possédant pas de pièce d'identité (accompagné d'un titre de haut niveau de confiance d'un parent)
- Des dispositifs d'identification électronique peuvent aussi être employés au sens du règlement eIDAS[4]

[4] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

Tous les autres documents d'identification permettent de créer une identité par défaut, mais en aucun cas de la valider ou de la qualifier.

En cas de divergences entre deux titres d'identités à haut niveau de confiance, il faut privilégier le passeport s'il fait partie des pièces présentées. Dans les autres cas, il faut prendre en compte les données du document le plus récent.

03.1.4 – L'appel au téléservice INSi

L'Identité Nationale de Santé de l'usager est recherchée, récupérée et/ou vérifiée par appel à un téléservice dédié nommé INSi.

Quand il est requis, l'appel à ce téléservice se fait par l'intermédiaire du système d'information en santé (SIS) et sous couvert d'une authentification de l'utilisateur (exemple : carte CPx physique ou procédure d'authentification dématérialisée).

L'interrogation du téléservice peut se faire selon deux modalités :

- Par l'intermédiaire de la carte Vitale (à privilégier)
- Par saisie des traits d'identité enregistrés localement ou transmis par un tiers (en utilisant à minima le nom de naissance, un des prénoms de naissance, le sexe et la date de naissance).

Parmi les informations contenues dans l'Identité Nationale de Santé renvoyées par le téléservice INSi, celles qui permettent l'identification de l'usager sont :

- Le matricule INS, constitué du numéro d'identification de l'individu au répertoire des personnes physiques (NIR ou NIA)
- Les traits INS, traits d'identité provenant de la base nationale de référence (SNGI) :
  - Le nom de naissance
  - Le(s) prénom(s) de naissance (séparés par des espaces)
  - La date de naissance
  - Le sexe
  - Le code géographique du lieu de naissance.

03.2 – Identification secondaire

L'identification secondaire correspond aux moyens mis en œuvre, à l'occasion de la prise en charge d'un usager physique par un professionnel, pour s'assurer de délivrer « le bon soin au bon patient ». Elle consiste notamment à contrôler, à chaque étape de sa prise en charge, la cohérence entre l'identité réelle de l'usager

et celle affichée sur les documents et outils de prise en charge (dossier physique ou informatique, prescription, étiquette, bon de transport, compte-rendu d'examen, etc.).

Différents moyens peuvent être mis en œuvre pour sécuriser cette étape, tels que

- La recherche de la participation active de l'usager à son identification, chaque fois que possible (« patient acteur de sa sécurité »), en lui demandant de décliner tout ou partie de son identité ;
- L'interrogation du patient par questions ouvertes (« Quel est votre nom de naissance ? », « Quel est votre prénom ? », etc.), en proscrivant l'utilisation de questions fermées de type « Vous êtes bien M/Mme UNTEL ? » ;
- La prise en compte, lorsqu'ils existent, des traits complémentaires (nom utilisé et prénom utilisé) afin d'employer les traits d'identité que l'usager utilise dans la vie courante lorsqu'on s'adresse directement à lui ;
- La mise en œuvre de dispositifs d'identification physique tels que la pose d'un bracelet, l'utilisation d'une photographie dans le dossier de l'usager, sous réserve du respect des droits du patient ;
- La vérification régulière de la concordance entre l'identité de l'usager pris en charge (déclinée ou vérifiée sur le dispositif d'identification physique) et celle relevée sur les documents (prescription, pilulier, étiquette, comptes rendus, résultats d'examens…).

04 Gestion des risques

La gestion des risques (GDR) est indissociable de la démarche d'amélioration continue de la qualité. Elle est classiquement distinguée en deux approches complémentaires selon le moment où l'action est menée :

- La GDR a priori, focalisée sur la prévention des risques évitables ;
- La GDR a posteriori, destinée à détecter et analyser les dysfonctionnements pour éviter qu'ils ne se reproduisent.

Sont introduits ci-après les principaux aspects relatifs à la politique à appliquer au niveau de chaque structure.

04.1 – 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.

Il s'agit d'un ensemble de composants (techniques et organisationnels) du SI qui garantissent la cohérence des données d'identité pour l'ensemble des logiciels métiers gérant des informations nominatives des personnes prises en charge.

Plusieurs domaines d'identification peuvent coexister au sein du système d'information de la structure. Ils sont tous reliés au référentiel d'identité qui est le serveur d'identités maître (généralement le logiciel de gestion administrative du malade / patient : GAM / GAP) sur lequel se raccordent les principales applications utilisées dans la structure. Le dossier patient informatisé (DPI), qui est une application totalement dépendante de la GAM / GAP en termes de gestion des identités, fait partie du même domaine d'identification que ce dernier.

D'autres logiciels, qui utilisent parfois une base de données d'identités propres et non reliée au référentiel principal, peuvent constituer des domaines d'identification distincts. Pour exemples :

- Gestion du bloc opératoire,
- Dossier d'anesthésie,
- Circuit de chimiothérapie.

04.2 – Recueil et enregistrement de l'identité

La qualité de l'identité numérique enregistrée dépend des modalités de récupération de celle-ci, selon que celle-ci est recueillie :

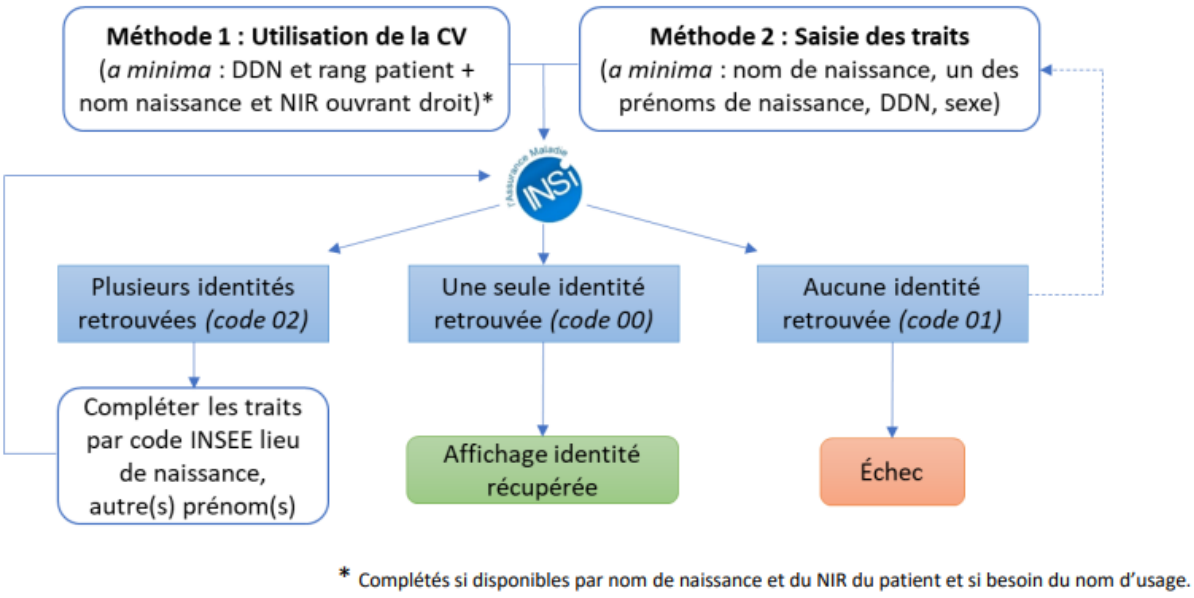
- Depuis l'appel au téléservice INSi
- A partir d'un document preuve, en fonction du type de document présenté
- A l'aide d'informations données de façon orale par l'usager, un proche ou tout autre intermédiaire
- Dans des conditions très dégradées (usager non accompagné inconscient, confus, non francophone…).

04.2.1– Utilisation du téléservice INSi

Les informations contenues dans l'Identité Nationale de Santé et renvoyées par le téléservice INSi par appel via carte vitale ou par traits peuvent permettre :

- Soit de créer directement une identité locale (s'il s'agit d'une première venue dans la structure),
- Soit de mettre à jour l'identité numérique existante en enregistrant les traits remontés par le téléservice INSi (améliorant par la même occasion le statut de confiance (cf. 02.4)).

Cependant, dans le deuxième cas, la récupération de l'identité numérique nécessite une concordance parfaite entre les bases nationales et locales : un contrôle de cohérence doit être fait avant tout remplacement des traits préalablement enregistrés dans la base locale.



* Complétés si disponibles par nom de naissance et du NIR du patient et si besoin du nom d'usage.

04.2.2– Autres modes de recueil de l'identité

Lorsqu'une pièce d'identité est présentée, les traits doivent être enregistrés tels qu'ils apparaissent sur le document fourni mais en respectant les règles de saisies définies dans le RNIV (cf. § 04.5 et Annexe § 08.1 de cette charte). S'il existe concordance entre le dispositif à haut niveau de confiance et la personne physique, l'identité peut être considérée comme « validée » (cf. § 02.4).

Dans tous les autres cas, l'identité numérique locale doit être sous le statut « provisoire », en attente de confirmation par tout moyen approprié (appel au téléservice, présentation d'un document validant…).

04.3 – Validation de l'identité

Habituellement, la procédure validation et/ou de qualification de l'identité se fait à l'occasion d'une venue de l'usager, en lui demandant de présenter un document attestant son identité ou en utilisant un dispositif d'identification à haut niveau de confiance.

04.4 - Recherche dans la base

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

Les critères de recherche utilisés se doivent donc d'être assez restrictifs pour retrouver le patient et relativement élargis afin de pouvoir éventuellement détecter des identités approchantes (doublon potentiellement existant).

Les principaux critères recommandés, non obligatoirement cumulatifs, pour la recherche sont :

- La date de naissance,
- Le nom de naissance,
- Le premier prénom de naissance.

En pratique, la recherche peut s'effectuer avec la date de naissance (en priorité) ainsi que les premières lettres du nom et du prénom de naissance.

Dans les cas où trop de résultats seraient retournés, l'utilisation prioritaire des autres traits stricts sera privilégiée.

04.5 - Règles de saisie pour la création d'une identité

Les règles de saisie sont applicables à tous les domaines d'identification de l'établissement de santé.

Cette identité doit être transcrite en caractères majuscules non accentués, sans signe diacritique et sans abréviation. Cependant, les tirets et apostrophes doivent être conservés. En revanche, les autres caractères diacritiques tels que « / » « , » doivent être remplacés par un espace (cf. RNIV 1 / Annexe § 08.1).

Pour les usagers, ne disposant pas de nom de naissance (champ vide sur la pièce d'identité, ou suite de X par exemple), il sera saisi SANSNOM, même s'il s'agit d'une suite de « X » ou tout autre mention pour signifier que la personne n'a pas de nom.

Pour les usagers, ne disposant pas de prénom de naissance (champ vide sur la pièce d'identité, ou suite de X par exemple), il sera saisi SANSPRENOM.

04.6 - Règles de rapprochement des identités

Le domaine d'identification (DI) est le périmètre au sein duquel chaque patient est représenté par un seul IPP. Chaque DI identifie le patient de façon propre avec un identifiant interne.

Le rapprochement est l'opération qui consiste à créer un couple d'identités issues de deux DI distincts et correspondant à une même personne physique. Les deux domaines d'identification sont alors dits « domaines rapprochés ».

Chaque structure de santé, au travers de son AGI ou de sa CIV (selon leurs missions qui leur sont attribuées respectivement : cf. § 01.4), doit :

- Désigner le service autorisé à rapprocher les identités (responsabilités)
- Définir les critères de rapprochement,
- Mettre en place une procédure et un mode opératoire pour fusionner les dossiers patients, en veillant à la qualification INS du dossier conservé,
- Garantir la traçabilité de toute action effectuée sur l'identité,
- Transmettre les informations relatives aux corrections à tous les DI et Professionnels concernés,
- S'assurer régulièrement de la qualité de la base de données des identités de chaque domaine d'identification (évaluation / identification - gestion des doublons et collisions).

04.7 - Règles d'impression des documents comportant une identité

Toutes les pièces du dossier d'un patient doivent être identifiées avec, au minimum, le nom de naissance, le sexe, le premier prénom de naissance et la date de naissance. Par ailleurs, si l'identité est qualifiée, le document devra comporter le matricule INS et sa nature (NIR ou NIA), sauf en cas d'espace réduit (type étiquette ou bracelet d'identification).

Si cela est applicable, il est recommandé d'y ajouter les informations relatives aux nom et prénom utilisés et, en tant que de besoin, à l'identifiant local de référence.

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

- Ce qui relève des traits stricts (en distinguant le nom de naissance du premier prénom),
- Ce qui relève des traits étendus/complémentaires.

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.

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 patient provenant d'une autre structure, doit être mise en œuvre afin d'informer la (ou les) structure(s) concernée(s).

04.8 - Règles de gestion des erreurs d'identité

Après signalement d'une erreur (alerte d'évènement indésirable selon procédure formalisée), la CIV est chargée de mettre en œuvre les mesures correctrices adaptées à l'événement, en relation avec les professionnels concernés. Les délais de mise en œuvre de ces actions dépendent de la nature de l'évènement.

Un ensemble de documents doivent être disponibles dans une GED et décrire :

- Les modalités de traitement des anomalies ou dysfonctionnements tels que la modification d'une erreur d'identité avérée, l'usurpation d'une identité le doublon d'identité, la collision,
- Les professionnels habilités à réaliser ces actions, le contexte et la traçabilité des actions,
- Le mode de communication et de suivi interne des actions correctives à mettre en œuvre,
- Le système de diffusion du signalement intra et inter structures afin de transmettre aux autres domaines d'identification concernés (cf. 04.6) les informations relatives à une anomalie à corriger,
- La conduite à tenir face à l'identification d'une erreur et les modalités d'information de la CIV lorsqu'un événement indésirable est associé à une mauvaise gestion de l'identité.

04.9 - Sécurité du système d'information

04.9.1 - Procédures

Une charte informatique (ou matrice d'habilitation) 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.

Des documents liés à l'éventuelle survenue d'une interruption de service en relation avec les données-patient doivent être mis à disposition du personnel impliqué.

Remarque : dans le cadre de la certification des établissements de soins, la maîtrise des risques numériques est mise en avant. Des indicateurs liés notamment aux attendus en termes de fiabilité, de confidentialité, de sécurité et de traçabilité du système d'information sont demandés (cf. Annexe § 08.1).

04.9.2 - 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 patient.

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

Dans le cas de la modification de l'identité, celle-ci sera réalisée au vu d'une pièce d'identité validante (cf. recueil d'identité § 04.2). Toute modification d'identité doit être diffusée, par des moyens garantissant une traçabilité aux acteurs concernés (messagerie interne, fiche d'évènement indésirable ou autre support). Dans ce cas, il est donc nécessaire de :

- Mettre en place une procédure pour rééditer les étiquettes et le bracelet d'identification,
- Garantir la traçabilité de toute action effectuée sur l'identité.

04.9.3 - Rapprochement et fusion

La possibilité de réaliser un rapprochement ou 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 et/ou une procédure.

La structure de santé prend les dispositions nécessaires pour organiser la réalisation des rapprochements / fusions dans les logiciels tiers lorsque l'opération n'est pas intégrée automatiquement.

Les opérations doivent être tracées (historisation informatique ou consigne manuelle) et transmises à tous les DI et Professionnels concernés.

04.9.4 - Identification des homonymes

La notion d'homonymie est définie comme la correspondance exacte entre plusieurs traits stricts (décrits au § 03.11).

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 la venue d'un patient avec des homonymes, il est important de prévoir comment diffuser une alerte aux différents correspondants (laboratoire, service d'imagerie, EFS, autres) pour limiter le risque d'erreur : contact téléphonique, alerte par message, étiquetage spécifique, etc.

04.9.5 - 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 patients 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.

05 Formation et sensibilisation

05.1 - Formation du personnel

La formation et la sensibilisation du personnel qu'il soit administratif ou technique, médical ou paramédical, doit être prévue par la structure de santé et prendre en compte tous les aspects de l'identitovigilance. Le périmètre de cette formation devra comprendre l'appréhension des procédures mises en place localement. Les modalités de réalisation devront comprendre à minima une intervention à l'arrivée dans la structure, sans oublier une remise à niveau régulière (formation continue).

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

NB : il est nécessaire de s'assurer par le biais d'évaluations que les personnels maîtrisent les applicatifs qu'ils utilisent et les procédures dégradées éventuelles.

05.2 - Sensibilisation des patients / usagers

Les patients et les accompagnants doivent être sensibilisés à l'identitovigilance, notamment par voie d'affichage, en particulier au niveau des accueils, secrétariats médicaux, admissions (panneaux ou vidéos pédagogiques), ainsi qu'au travers du livret d'accueil. Ils doivent être incités à participer à leur identification et à vérifier les informations utilisées pour les identifier. Le même type d'informations doit aussi être diffusé sur le site internet et/ou de prise de rendez-vous de la structure.

Par ailleurs, les patients 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), et de la nécessité de mesures de vérification à chaque étape des procédures de soins.

05.3 - Respect des droits des patients / RGPD

Les structures de santé se doivent de respecter les principes des chartes des patients hospitalisés.

Ces chartes rappellent les droits des patients 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 ;
- D'être informé du partage des données d'identité au niveau régional.

Le traitement des données à caractère personnel se doit également de respecter le RGPD (Cf. Annexe § 08.1).

06 Indicateurs qualité

La mise en place d'indicateurs qualité permet d'évaluer/améliorer la prévention et la gestion des risques, et à terme la performance du système : caractérisation et quantification des problèmes de sécurité en lien avec l'identité des patients et vérification de l'efficacité des mesures correctives.

A minima, les éléments à analyser et recommandés sont les suivants :

- Nombre / taux de doublons créés ou détectés
- Nombre de fiches Evènements Indésirables / signalement créées (identification primaire / secondaire)
- Nombre de modifications d'identités réalisées
- Taux d'identités INS récupérées / qualifiées
- Nombre / taux de personnel formé (par catégorie de professionnels)

07 Procédures

Certaines procédures opérationnelles doivent être formalisées en fonction de la structure aux fins de bien cadrer l'application correcte des règles d'identitovigilance, et doivent apparaître en annexe d'application de cette charte.

Cette liste (non exhaustive) est à adapter en fonction du type de structure, de sa taille, des prises en charge concernées et des risques identifiés.

Exemples de procédures en relation avec l'organisation des soins :

- Recherche d'un patient dans la base ;
- Identification primaire à l'accueil de l'usager ;
- Patient dans l'incapacité de décliner son identité ;
- Suspicion d'usurpation d'identité ;
- Nouveau-nés ;
- IVG ;
- Accouchement sous X ;
- Confidentialité et anonymat ;
- Usager transgenre
- Patient sous main de justice ;
- Situation Sanitaire Exceptionnelle ;
- Identification secondaire avant tout acte de soin ;
- Pose et utilisation d'un bracelet d'identification ;
- Correction et rapprochement d'identités (et/ou fusion + collision) ;
- Déclaration et gestion des EI en lien avec l'identitovigilance ;
- Contrôle qualité des bases d'identités ;
- Gestion en cas de panne du système d'information ;
- Gestion des identités dans les logiciels non ou incomplètement interfacés ;
- Gestion des habilitations.

08 Annexes

08.1 - Références réglementaires et techniques

- Circulaire DHOS/E1/DGS/SD1B/SD1C/SD4A/2006/90 du 2 mars 2006 relative aux droits des personnes hospitalisées et comportant une charte de la personne hospitalisée : https://www.legifrance.gouv.fr/download/pdf/circ?id=10571 / https://solidarites-sante.gouv.fr/IMG/pdf/flyer_a5_couleur.pdf
- Guide méthodologique de mise en œuvre de l'identité patient au sein des groupements hospitaliers de territoire (ASIP Santé, 2018) : https://esante.gouv.fr/media/1823
- Instruction **abrogée** DGOS/MSIOS no 2013-281 du 7 juin 2013 relative à l'utilisation du nom de famille (ou nom de naissance) pour l'identification des patients dans les systèmes d'information des structures de soins : https://solidarites-sante.gouv.fr/fichiers/bo/2013/13-08/ste_20130008_0000_0161.pdf
- Manuel de certification des établissements de santé pour la qualité des soins / version octobre 2020 : https://www.has-sante.fr/upload/docs/application/pdf/2020-11/manuel_certification_es_qualite_soins.pdf
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) : https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- Instruction générale relative à l'état civil du 2 novembre 2004 : https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000001073693
- Note d'information N° DGOS/PF2/PF5/2020/202 du 18 novembre 2020 relative à la publication du référentiel national d'identitovigilance des acteurs de santé – principes généraux et mise en œuvre dans les établissements de santé : Bulletin officiel Santé - Protection sociale - Solidarité n° 2021/1 du 29 janvier 2021 (solidarites-sante.gouv.fr)

08.2 - Sites externes de référence

- Site de l'Agence du Numérique en Santé (ANS) sur l'Identité Nationale de Santé (INS) :

  Identité Nationale de Santé (INS) | esante.gouv.fr

- Site du ministère de la santé et de la prévention, pages consacrées à l'identitovigilance :

  Identitovigilance - Ministère de la Santé et de la Prévention (solidarites-sante.gouv.fr)

08.3 - Glossaire

Cf. Référentiel National d'IdentitoVigilance 1 (RNIV1) – Principes d'identification des usagers communs à tous les acteurs de santé - Annexe 2 : terminologie et définitions.

Groupement d'Intérêt Public
e-santé Occitanie

www.esante-occitanie.fr

Siège social
10 rue des trente-six Ponts
31400 Toulouse
05 67 20 74 00