Agence Régionale de Santé
Hauts-de-France

CHARTE REGIONALE D'IDENTIFICATION DE L'USAGER DANS SON PARCOURS DE SANTE

Version 1.8

HISTORIQUE DES REVISIONS

VERSION	DATE DE MISE A JOUR	DESCRIPTION DES EVOLUTIONS	AUTEUR
V0.1	17.01.2019	Création de la charte - Définition des composantes de l'identitovigilance régionale	Groupe de travail régional
V0.2	06.02.2019	Modifications -Relecture de la Charte	Groupe de travail régional
V0.3		Amendements sur la forme	Sant& Numérique Hauts-de-France
V0.4	25.02.2019	Correctifs - Relecture de la Charte	Groupe de travail régional
V1.0	05.03.2019	Validation de la charte (hors périmètre de la gouvernance)	Groupe de travail régional
V1.1	14.05.2019	Complétion du volet gouvernance	Groupe de travail régional
V1.2	16.05.2019	Amendements sur la forme	Sant& Numérique Hauts-de-France
V.1.3	25.05.2019	Validation du contenu de la charte	Groupe de travail régional
V1.4	18.06.2019	Relecture juridique (RGPD) et correctifs	Sant& Numérique Hauts-de-France
V1.5	05.08.2019	Correctifs	Sant& Numérique Hauts-de-France
V1.6	27.01.2020	Modification du volet gouvernance et intégration code INSEE	ARS
V1.7	20.02.2020	Correctifs	Sant& Numérique Hauts-de-France
V1.8	09/03/2020	Validation	ARS

Rédacteur(s) : Groupe de travail régional
Responsable : **Sant& Numérique Hauts-de-France**
Pièce(s) jointe(s) :
Diffusion :

Table des matières

1. Introduction

1. Contexte et enjeux

L'identification de l'usager est un préalable indispensable pour assurer la continuité, la qualité et la sécurité de la prise en charge des usagers, ainsi que la coopération entre les professionnels de santé, notamment dans le cadre des parcours de soins, de santé et de vie. En effet, l'identification fiable de la personne prise en charge est indispensable pour :

- Éviter le risque d'erreur médicale associé à une mauvaise identification du patient ;
- Permettre le partage des éléments du dossier du patient (données, comptes-rendus, images, ...) entre les professionnels de santé concernés, ces derniers de plus en plus nombreux ;
- Supporter les attentes légitimes de l'usager en termes de qualité et sécurité des soins et permettre l'engagement de l'usager comme acteur de sa prise en charge tout au long de son parcours de santé.

Or, à ce jour, un usager peut être identifié différemment dans les systèmes d'information des multiples structures qui composent le système de santé.

L'enjeu est donc de pouvoir disposer d'une organisation et d'une infrastructure qui permettent de considérer chaque patient comme une personne unique, afin de pouvoir « chaîner » ses informations tout au long du parcours de santé. Cette organisation est en cohérence avec la stratégie régionale d'identitovigilance définie par l'agence régionale de santé (ARS) Hauts-de-France et les recommandations portées par l'agence nationale d'appui à la performance (ANAP)(voir annexe 1).

La charte d'identification de l'usager dans son parcours de santé entre dans une logique de protection des données à caractère personnel dans l'environnement numérique de prise en charge et de continuité des soins. A ce titre, la charte s'inscrit dans une logique de protection des données dès la conception (Privacy by design), ainsi que par défaut (Privacy by default) en reposant sur des mesures techniques et organisationnelles strictes. La charte intègre par conséquent les principes et exigences du 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 (RGPD) ainsi que celles de la loi du 6 janvier 1978 relative à l'informatique et aux libertés.

1.1. Objectifs de la charte régionale d'identitovigilance

La politique menée par l'Agence régionale de santé (ARS) Hauts-de-France pour assurer la bonne identification des usagers à toutes les étapes de leur prise en charge sur le territoire poursuit les objectifs suivants :

- 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 ;
- Réduire le risque d'erreurs d'identification des personnes prises en charge ;
- 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 ;
- 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 ;
- Sécuriser le rapprochement d'identité entre structures différentes ;
- Permettre une communication continue et partagée entre établissements en matière d'identitovigilance ;
- Encourager le développement d'interfaces logicielles conformes aux exigences en termes d'identitovigilance.

La charte régionale d'identification de l'usager dans son parcours de santé, fruit d'un consensus régional, est un document pratique permettant de mettre en œuvre la politique régionale. Toute structure souhaitant être raccordée au système d'identification régionale s'engagera à respecter la charte. En effet, cette charte marque l'engagement des parties prenantes au respect de principes directeurs en matière de gestion d'identité des personnes.

A partir de la charte régionale d'identification de l'usager, la structure de santé peut élaborer sa propre charte en reprenant les principes obligatoires et les procédures, ou mettre à jour une charte existante et ainsi converger vers l'identification partagée du patient au niveau régional.

La charte d'identification de l'usager précise les principes suivants retenus au niveau régional :

- Le patient est identifié d'une manière unique au sein d'une structure de santé ;
- Les traits personnels du patient sont repérés afin de les rendre communs au niveau régional et faciliter les rapprochements entre systèmes ;
- Un ensemble de fonctions de base de gestion de l'identification des patients dans les systèmes d'information est défini au niveau régional ;
- Les bonnes pratiques procédurales sont partagées au niveau régional.

La charte pose des règles simples et applicables pour mettre en place un cadre commun connu de tous dans l'objectif de sécuriser le parcours de santé de l'usager.

Le Serveur de rapprochement d'identité (SRI) régional sera fondé sur les orientations définies par la présente charte et tiendra compte des différences de pratiques constatées entre les structures de la région.

1.2. Périmètre

Dans une perspective d'homogénéisation des pratiques dans le temps, la politique régionale d'identitovigilance s'applique à tous les modes de prise en charge et d'accueil dans les secteurs sanitaire et médico-social.
Les acteurs concernés sont :

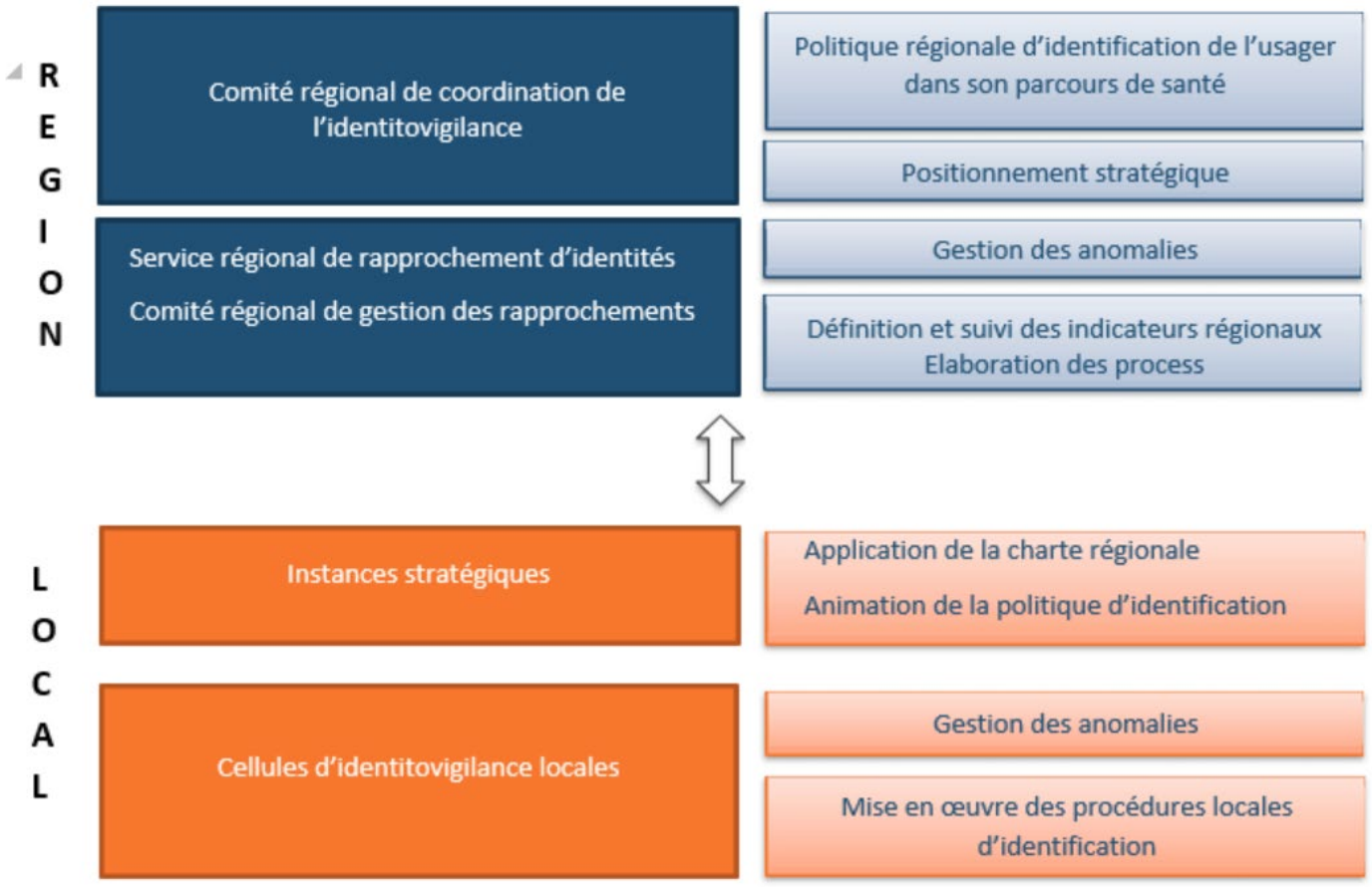
- L'usager, acteur de sa santé, et sa personne de confiance ;
- Les professionnels de santé assurant la prise en charge ;
- Les autres professionnels qui interviennent sur tout ou partie des données médico-socio-administratives des usagers.

2. Gouvernance régionale de l'identitovigilance en Hauts- de- France

2.1. Gouvernance régionale de l'identitovigilance

Les instances ont pour rôle de définir et de mettre en œuvre la charte régionale d'identification de l'usager dans son parcours de santé dans la région Hauts-de-France. Elles accompagnent et animent la diffusion de la charte dans les structures de santé afin d'améliorer la qualité de l'identification de l'usager. On distingue :

- Le comité régional de coordination de l'identitovigilance
- Le comité régional de gestion des rapprochements
- Le service régional de rapprochement d'identités (SRRI)



2.1.1. *Le comité régional de coordination de l'identitovigilance*

Le comité régional de coordination de l'identitovigilance est une instance stratégique définissant la politique d'identitovigilance régionale dans toutes ses composantes. Elle se réunit a minima trois fois par an. Elle est présidée par l'ARS Hauts-de-France et animée par le RREVA (Réseau régional de vigilances et d'appui).

Sa composition est la suivante :

- Deux représentants de l'ARS (un représentant de la Direction de la Sécurité sanitaire et de la santé environnementale et un représentant de la Direction de la Stratégie et des Territoires) ;
- Deux représentants du RREVA ;
- Un représentant de Sant& Numérique Hauts-de-France au titre du Service régional de rapprochement d'identités.

Les missions du comité régional de coordination d'identitovigilance sont les suivantes :

- Elaborer/Emettre un avis sur la stratégie régionale de gestion de l'identification de l'usager ;
- Rédiger, valider, mettre à jour la charte régionale d'identification ;
- Contribuer à faire adhérer les structures de santé et les fournisseurs de technologies à la charte régionale ;
- Valider les actions de communication et de sensibilisation autour de la charte régionale

et des procédures (bonnes pratiques notamment) et produire ou mettre à jour si besoin les supports nécessaires en coordination avec le RREVA;
- Valider et suivre les indicateurs régionaux et le bilan régional de la qualité de l'identification du patient ;
- Valider les critères de raccordement d'un domaine d'identification (DI) ;
- Déclencher les plans d'actions lorsque sont relevées des anomalies graves voire stopper la production en cas d'alerte levée par le SRRI.

2.1.2. *Le comité régional de gestion des rapprochements*

Le comité régional de gestion des rapprochements est une instance représentative des professionnels issus de l'ensemble des structures de santé de la région Hauts-de-France. Sa composition reflète la pluri-disciplinarité des référents-métiers impliqués dans la gestion des rapprochements à l'échelon régional. Cette structure est liée à la mise en œuvre technique du programme Prédice.

Il est composé d'un titulaire et d'un suppléant :

- représentant chacun des serveurs de rapprochement d'identités (SRI) mis en place dans le cadre de Prédice ;
- représentant chacun des acteurs utilisant directement le SRI à l'échelon régional (URPS ; fédérations médico-sociales…) ;
- représentant l'Union régionale des associations agréées des usagers du système de santé;
- représentant le RREVA.

Les missions du comité régional de gestion des rapprochements sont les suivantes :

- établir les process d'échange entre les différents SRI et structures impliquées ;
- valider la charte régionale de rapprochement d'identité ;
- rédiger, valider, mettre à jour les procédures de rapprochement ;
- coordonner les communications auprès des éditeurs pour faciliter de futures évolutions ;
- prendre en compte les difficultés rencontrées par les acteurs et proposer au comité de coordination régional de l'identitovigilance des solutions techniques ou organisationnelles permettant de faciliter les rapprochements.

Tout nouvel acteur intervenant dans la politique régionale d'identitovigilance sera amené à intégrer le comité régional de gestion des rapprochements en tant que membre à part entière ou en tant qu'invité. Les dispositions régissant l'intégration de ces nouveaux membres seront définies par le comité lui-même. Chaque structure dégage les temps dédiés nécessaires au bon fonctionnement de l'instance.

2.1.3 *Le service régional de rapprochement d'identités*

Le service régional de rapprochement d'identités (SRRI) est une instance opérationnelle de Sant& Numérique Hauts-de-France. Son activité est quotidienne.

Sa composition est la suivante :

- Un responsable
- Un chargé de mission régional identitovigilance
- Un médecin référent.

Le service régional de rapprochement d'identités a pour missions :

- Assurer au quotidien la gestion des anomalies et mettre en œuvre toute action provisoire dans l'attente d'un positionnement du comité régional de gestion des rapprochements ;
- Préparer les travaux à destination du comité régional de coordination de l'identitovigilance ;
- Définir et assurer la consolidation des indicateurs régionaux de qualité (sécurité mise en œuvre dans les structures de santé/Audit du référentiel d'identité régional) ;
- Identifier les besoins d'évolution des chartes au vu de l'analyse des indicateurs ;
- Mettre en place des alertes auprès des acteurs et du RREVA dans le cadre du suivi des indicateurs ;
- Définir une cartographie des risques d'identitovigilance régionale et assurer un soutien aux structures locales dans la définition et la mise en place de cette cartographie en lien avec le RREVA.
- Piloter la gestion des risques lors du rapprochement des identités dans le SRI en animant le réseau des référents identitovigilance SRI des cellules d'identitovigilance locales ;
- Elaborer le rapport annuel de la qualité de l'identification de l'usager au niveau régional & le rapport annuel de la SRRI ;
- Traiter des anomalies fonctionnelles constatées sur des flux identités en Phase de Raccordement d'un Domaine d'identification (DI) ou lors du changement d'une Gestion administrative des malades (GAM) ou d'une évolution majeure ;
- Rédiger/ mettre à jour la charte régionale de rapprochement des identités qui sera validée par le comité régional de gestion de rapprochements ;
- Contribuer à la validation d'un raccordement et assister les acteurs lors de ce raccordement ;
- Faire des analyses d'impact en amont des évolutions logicielles;
- Assister les acteurs lors du changement d'une GAM ou d'une évolution majeure ;
- Assurer une veille réglementaire.

2.2 Gouvernance locale de l'identitovigilance

La charte régionale d'identification de l'usager a vocation à s'appliquer dans l'ensemble des structures de santé de la région des Hauts-de-France et à toutes les prises en charge.

La structure reste décisionnaire dans la déclinaison locale de la charte régionale. Une gouvernance stable de l'identitovigilance doit néanmoins pouvoir s'appuyer sur une instance stratégique et une instance opérationnelle.

L'instance stratégique a vocation à être positionnée à l'échelon GHT (voire à un échelon supérieur incluant la psychiatrie, le secteur privé, le médico-social et/ou le monde libéral) afin de favoriser la mise en œuvre d'une politique locale d'identitovigilance. Elle s'assurera de la mise en œuvre d'une charte de rapprochement du GHT prévoyant notamment les modalités de délégation au sein de celui-ci.

L'instance opérationnelle comprend des professionnels de l'identitovigilance. Ces professionnels sont les correspondants de l'instance stratégique et du service régional de rapprochement d'identité (SRRI). A ce titre, ils doivent pouvoir bénéficier régulièrement de formations relatives à l'identitovigilance.

Ces instances doivent avoir défini des procédures permettant la levée d'alerte suite à des anomalies d'identitovigilance au sein de leur structure et assurent un suivi des indicateurs.

3 Structuration de l'identification

3.1 Principes de qualification de l'identité

La confiance à accorder à l'identité recueillie doit être évaluée en fonction des documents pris en compte lors de l'enregistrement de l'usager.

3.1.1 Documents permettant de valider une identité

L'identité est « **validée** » lorsqu'elle est relevée à partir d'un document d'identité européen officiel comportant les traits stricts :

- La carte nationale d'identité (CNI)[1] ;
- Le passeport ;
- Le titre de séjour ;
- L'extrait d'acte de naissance ;
- L'acte de naissance pour les nouveau-nés ;
- Le livret de famille, pour les mineurs ne possédant pas de document d'identité ;
- 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 ;
- Le permis de conduire ANTS[2].

Pour toute identité validée, le fondement de la validation doit être tracé par la saisie d'un commentaire (type de document présenté/date/professionnel à l'origine de la validation) ou, à défaut, par la conservation d'une copie du document présenté. La conservation des documents ne pourra se faire que sur une durée de temps limitée et dans le cadre d'une procédure établie (cf. infra 3.1.4).

[1] Depuis le 1er janvier 2014, la durée de validité de la carte nationale d'identité est passée de 10 à 15 ans pour les personnes majeures (plus de 18 ans). L'allongement de cinq ans pour les cartes d'identité concerne :

- Les cartes d'identité sécurisées (cartes plastifiées) délivrées entre le 2 janvier 2004 et le 31 décembre 2013 à des personnes majeures ; La date de fin de validité mentionnée sur ces cartes est donc désormais fausse, il faut y ajouter 5 ans.
- Les nouvelles cartes d'identité sécurisées (cartes plastifiées) délivrées à partir du 1er janvier 2014 à des personnes majeures ;

Cette prolongation ne s'applique pas aux cartes nationales d'identité sécurisées pour les personnes mineures dont la validité est toujours de 10 ans.

[2] Le permis de conduire est-il une pièce d'identité officielle ? Vérifié le 21 juin 2018 - Direction de l'information légale et administrative (Premier ministre), sur la base de la Réponse ministérielle du 26 octobre 2010 relative à la réglementation en matière de pièces d'identité. Disponible sur : https://www.service-public.fr/particuliers/vosdroits/F11860

« Oui, le permis de conduire est une pièce d'identité officielle, car il est délivré par l'État français. Il peut permettre de justifier son identité à condition que la photographie d'identité soit ressemblante […] Par ailleurs, le permis n'a pas la même valeur que la carte nationale d'identité ou le passeport, qui sont les seuls à certifier à la fois l'identité et la nationalité de leur titulaire. »

3.1.2 *Identité provisoire*

L'identité est **« provisoire »** tant qu'un document officiel d'identité n'a pas été produit. Il est rappelé que les documents de justice ainsi que les données enregistrées sur la carte Vitale ne permettent pas de qualifier l'identité d'un patient et ne constituent donc pas des pièces officielles d'identités.

En l'absence de documents permettant de valider une identité, il peut aussi être proposé d'associer plusieurs documents afin d'améliorer le niveau de confiance à accorder, néanmoins l'identité ne sera pas « validée ».

3.1.3 *Discordance entre documents d'identité*

En cas de discordances entre documents permettant de valider une identité, c'est le document d'identité ayant le plus fort niveau de confiance qui doit être pris en compte. Une classification est proposée ci-dessous, à moduler en fonction de la date de chacun des documents, de la présence de photographie récente ou de tout autre élément de contexte complémentaire.

Libellé	Confiance
• La carte nationale d'identité européenne (CNI)	Très forte
• Le passeport	
• L'extrait d'acte de naissance	Forte
• Le livret de famille, pour les mineurs ne possédant pas de document d'identité	
• Le titre de séjour	Moyenne
• Le permis de conduire ANTS	
• 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	

Remarques :

- *Il convient dans tous les cas d'inviter l'usager à faire corriger les données erronées par l'organisme d'état civil compétent. La rectification des erreurs est un droit que l'usager doit faire valoir auprès du service d'état civil de son domicile ou de son lieu de naissance (art. 60 du code civil modifié par la loi n°2016-1547 du 18 novembre 2016 - art. 56).*
- *Après correction, l'établissement est invité à garder une trace des changements d'état civil (dans le respect du Règlement* général de la protection des données, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 201, *cf. 3.1.3)*

3.1.4 *Vigilance sur la conservation des documents d'identité*

L'article 5 du règlement général de protection des données (RGPD) prévoit que les données à caractère personnel sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

La saisie par les services opérationnels d'un commentaire attestant du document d'identité présenté doit donc être privilégiée à la conservation du document d'identité. Si le processus établi dans la structure prévoit néanmoins la conservation d'une copie des documents présentés, une procédure spécifique doit définir les conditions et la durée de conservation ainsi que les modalités de destruction.

3.2 Traits d'identification retenus

3.2.1 *L'INS comme identifiant pivot*

L'INS est l'identifiant pivot obligatoire pour l'échange et le partage des données de santé et documents médicaux. La loi consacre le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR, numéro d'inscription au répertoire national d'identification des personnes physiques, plus communément appelé « numéro de sécurité sociale ») comme identifiant national de santé (INS) des personnes pour leur prise en charge à des fins sanitaires et médico-sociales. L'INS est soit le NIR soit le NIA (numéro identifiant d'attente) pour les personnes en attente d'immatriculation associé à des traits d'identité.

En effet, un identifiant seul n'apportant pas les garanties minimales nécessaires à l'identitovigilance, l'Etat fournit un accès aux données de références associées à l'INS (Nom de famille, prénoms, sexe, date de naissance, lieu de naissance) par la mise à disposition par la caisse nationale d'assurance maladie de téléservices de recherche et de vérification de l'INS et des traits de référence associés. La bonne association entre l'INS, les traits de référence et la personne prise en charge est effectuée au cours d'une procédure d'identitovigilance propre à la profession de prise en charge qui accueille l'usager. L'INS et les traits sont dits qualifiés lors qu'ils sont recueillis à l'occasion d'une procédure d'identitovigilance et qu'ils sont récupérés ou vérifiés grâce à l'appel aux téléservices mis en œuvre par l'assurance maladie.

Dans l'attente de la mise en place des téléservices de recherche et de vérification de l'INS et des traits de références associés, les professionnels s'attachent à identifier les usagers **sur la base de l'INS-C ou du numéro de sécurité sociale associés aux traits stricts définis ci-dessous.**

La procédure d'identitovigilance retient, en effet, trois catégories de traits d'identifications : les traits stricts, les traits étendus et les traits complémentaires.

3.2.2 *Les traits stricts*

Les traits stricts sont des données stables d'état civil, vérifiables à partir de documents d'identité officiels comportant ou non une photographie.

Les traits stricts sont obligatoires. Ils sont utilisés comme critères déterminants pour rechercher des dossiers antérieurs ou pour rapprocher des identifiants.

Les acteurs du médico-social, de l'ambulatoire ou de ville n'ayant pas nécessairement la capacité à appliquer l'ensemble des principes de la charte, sont invitées à apporter a minima la plus grande vigilance sur la saisie de ces traits stricts.

La charte régionale d'identification retient comme traits stricts :

- Le nom de naissance (nom de famille selon la dénomination de l'état civil) ;
- Le premier prénom de naissance figurant sur le document officiel d'identité (qui peut être composé) ;
- La date de naissance ;
- Le genre ;
- Le lieu de naissance : code INSEE de la commune de naissance pour un ressortissant français /code INSEE du pays pour un étranger.

En l'état actuel, tous les acteurs ne sont pas en mesure de renseigner les éléments définis ci-dessus.
Dans une démarche d'accompagnement au changement, le serveur de rapprochement d'identités mis en place à l'échelon régional propose, dans un premier temps, des mécanismes de compensation.
En pratique, pour qu'un rapprochement puisse s'effectuer de manière automatique, il faudra disposer a minima de cinq données.
Les 4 premières sont : nom de naissance, premier prénom de naissance, date de naissance et genre ;
La cinquième peut être, au choix :

- *Le numéro de sécurité sociale ;*
- *L'INS-c ;*
- *Le code INSEE ou code postal du lieu de naissance couplé au 2ème prénom*

N.B : une vérification est effectuée afin de s'assurer de la cohérence entre le numéro de sécurité sociale et la date de naissance de la personne.

Une décision de justice peut modifier certaines données. Il est donc important de disposer d'un document d'identité récemment mis à jour. En effet, en cas de discordance entre les déclarations de l'usager et les données écrites fournies, le document le plus récent fera foi.

Remarques :

- *L'adoption plénière entraîne la modification du nom de naissance, sans lien avec le précédent. En cas d'adoption simple, le nom du ou des adoptants peut s'ajouter ou remplacer le nom de l'adopté.*
- *En France, tout requérant peut demander à la mairie du domicile ou du lieu de naissance de lui communiquer les : nom de naissance, prénoms, date et lieu de naissance, ainsi que la dernière situation matrimoniale d'une personne.*

Une attention particulière devra être portée sur les règles de saisie liées aux prénoms (premier prénom et prénoms suivants, cf. infra).

ⓘ Difficultés relatives au prénom de naissance

Prénoms composés

Sur un document d'identité français, une virgule sépare normalement les prénoms. Le premier prénom peut être composé. Les prénoms du nom composé sont alors habituellement regroupés par un tiret. Cependant, cette règle n'est pas obligatoire. Certains prénoms composés utilisent l'espace comme séparateur. C'est notamment le cas pour certains prénoms d'origine étrangère qui contiennent des préfixes (par exemple ould, ben walid, abou, umm…) ou des mots de liaison (par exemple dos, das, da, della…)

Quelques exemples :

Règles	*Exemples*	*Informations à saisir dans le SI*
Avec une virgule on enregistre le(s) prénom(s) précédant celle-ci	• *Jean, Pierre, Edouard, Michel*	• *Enregistrer JEAN*
	• *Jean Pierre, Edouard, Michel*	• *Enregistrer JEAN PIERRE*
Avec un tiret reliant les 2 premiers prénoms, on enregistre le prénom composé	• *Jean-Pierre, Edouard, Michel*	• *Enregistrer JEAN-PIERRE (ou JEAN PIERRE, cf. 4.2)*
	• *Jean-Pierre Edouard Michel*	• *Enregistrer JEAN-PIERRE (ou JEAN PIERRE, cf. 4.2)*
En l'absence de virgule, on n'enregistre que le premier prénom de la liste	• *Jean Pierre Edouard Michel*	• *Enregistrer JEAN*
	• *Jean Pierre*	• *Enregistrer JEAN (sauf exception : cf. encadré ci-dessous)*
Quelques exceptions sur des prénoms d'origine étrangère	• *Walid, Mahamoud*	• *Enregistrer WALID*
	• *Ben Mohamed*	• *Enregistrer BEN MOHAMED*
	• *Ould Ahmed*	• *Enregistrer OULD AHMED*
	• *Thi Loan*	• *Enregistrer THI LOAN*
	• *Alcida Dos Anjos*	• *Enregistrer ALCIDA DOS ANJOS*

Contestation d'enregistrement du premier prénom

S'agissant d'un trait strict, il n'est pas possible de déroger à la règle d'enregistrement du premier prénom de naissance. A défaut de produire un autre document d'identité de haut niveau de confiance permettant de certifier l'identité souhaitée (cf. 3.1.1), c'est bien celui enregistré sur le document officiel d'identité présenté qui est à enregistrer.

Exemples :

- *Jean Pierre, Edouard → enregistrer JEAN PIERRE*
- *Jean Pierre → enregistrer JEAN (règle générale) ou JEAN PIERRE (avec documentpreuve)*

Attention : la possibilité de porter un prénom composé sans tiret de séparation peut parfois poser problème lorsqu'il n'est pas suivi d'une virgule sur le document. L'usager (ou un de ses ayants-droit) doit être invité à faire modifier ses papiers auprès de l'état civil, seule possibilité pour que le changement soit effectivement pris en compte.

Enregistrement d'un prénom d'usage (ou alias)

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

3.2.3 *Les traits étendus*

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

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

La charte régionale d'identification retient comme traits étendus :

- Le nom d'usage (inclus nom marital) ou l'alias d'usage ;
- Les prénoms secondaires ;
- Le prénom d'usage (officiel ou habituellement utilisé par l'usager) ou l'alias d'usage ;
- Le nom et prénom de la mère ;
- Le nom et prénom du père ;
- Le code postal du lieu de naissance ;
- L'adresse mail personnelle ;
- Le numéro de téléphone portable personnel.

La saisie des traits étendus reste facultative. Néanmoins, la saisie d'un maximum d'informations renforce la procédure d'identitovigilance et facilite les rapprochements automatiques pour les structures de santé s'appuyant sur un serveur de rapprochement.

ⓘ Difficultés relatives au nom d'usage

Enregistrement du nom d'usage (ou alias)

Le nom d'usage, qu'il soit précédé de « époux/se de », « divorcé/e de », « veuf/ve » (ou leurs équivalents comme « Ep. », « Div. », « Vve ») doit être enregistré tel qu'il apparaît sur le document d'identité présenté dans le champ correspondant (cf. 3.2), sans la mention qui le précède.

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

Contestation d'enregistrement du nom d'usage (ou alias)

Certaines personnes divorcées présentent des documents d'identité mentionnant encore leur nom marital. L'enregistrement des identifiants est à réaliser sans déroger à la règle générale pour les traits stricts, en recopiant les mentions portées sur le document d'identité présentée. Néanmoins s'agissant d'un trait étendu sa saisie reste, comme indiqué ci-dessus, facultative.

3.2.4 *Les traits complémentaires*

Les traits complémentaires sont des informations supplémentaires pouvant être utilisées pour faciliter le rapprochement d'identité entre deux dossiers lorsque les éléments précédents ne sont pas suffisants ou lorsqu'il existe des doutes d'identité.

Ces traits complémentaires peuvent être notamment :

- L'arrondissement de naissance ;
- L'adresse de résidence de l'usager ou de l'assuré ;
- La profession ;
- Le numéro de téléphone fixe;
- Le nom des personnes en relation (parent, enfant, conjoint, personne de confiance…) ;
- Le médecin traitant ;
- Le document d'identité utilisé ;
- L'IPP ou tout autre identifiant local.

Dans certaines situations, il peut s'avérer nécessaire de confronter des traits complémentaires susceptibles d'être couverts par le secret médical. Seuls les professionnels de santé intervenant dans le cadre du parcours de soin de l'usager seront alors habilités à accéder au dossier médical de la personne afin d'émettre un avis sur son identité. Cette démarche est mise en œuvre dans le cadre d'une procédure spécifique.

3.2.5 *Cas particuliers*

a) Identités sensibles

Les identités traitées dans le cadre des statuts spécifiques de prise en charge doivent faire l'objet de procédures internes spécifiques (cf. 4.4).

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

b) Certificats de décès

Les règles d'identitovigilance s'appliquent également lors de la rédaction des certificats de décès.

Il est important de vérifier que les données renseignées correspondent bien aux champs attendus (avec une vigilance particulière sur le nom de naissance).

3.2.6 *Point de contact unique en cas de difficultés d'application de la charte*

Pour toute difficulté d'application de la charte d'identification régionale, les structures appliquant cette charte peuvent entrer directement en contact avec le service régional de rapprochement d'identités et le comité régional de coordination de l'identitovigilance : identitovigilance@esante-hdf.fr

4. Gestion de l'identité patient

4.1 Référentiel d'identité

Les établissements 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.

Les autres structures sont invitées à formaliser autant que possible la gestion des cas complexes.

4.1.1 *Un référentiel unique d'identité par structure*

Chaque structure doit disposer d'un référentiel unique d'identités. Ce référentiel doit s'inscrire dans le respect du cadre des projets de e-santé (cf. 6.2)

Au sein des établissements 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.

Le SI garantit la cohérence des données d'identité pour l'ensemble des logiciels métiers gérant des informations nominatives des personnes prises en charge.

4.1.2 *Un enregistrement réalisé par des professionnels habilités*

L'enregistrement de l'identité de l'usager dans le SI est réalisé sous la responsabilité de professionnels habilités à le faire. Cette opération est réalisée après contrôle immédiat ou secondaire des documents d'identité (cf. 3.1).

4.1.3 *Une recherche préalable impérative*

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.

Cette démarche fait l'objet d'une procédure mettant en avant les principes suivants :

- La recherche se fait prioritairement sur la date de naissance et, s'affine sur les autres traits stricts ;
- La recherche ne doit jamais se faire sur l'identité complète (nom, prénom, date de naissance) ;
- Les noms d'usage doivent également être recherchés le cas échéant.

4.2 Règles de saisie

4.2.1 *Utilisation des tirets, apostrophes et caractères spéciaux*

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

La consigne figurant dans l'instruction DGOS/MSIOS du 7 juin 2013 relative à l'identification des patients, de remplacer tirets et apostrophes par des espaces a été édictée pour pallier l'incapacité de certains logiciels à traiter ces caractères lors des opérations de recherche et de rapprochement. Les logiciels métiers ont aujourd'hui évolué et sont en mesure de remplacer virtuellement les caractères de ponctuation, rendant obsolète cette consigne.

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

- **Méthode préconisée : Recopier le plus fidèlement possible les traits des documents présentés, dans la mesure où le système d'information est en capacité de supprimer ces caractères lors d'opérations de recherche et de rapprochement ;**
- Remplacer les caractères de ponctuation par des espaces si la configuration locale n'offre pas de possibilité de paramétrage avancé de ces opérations.

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

Si la configuration locale ne permet pas de saisir les caractères spéciaux, la règle est de transformer ceux-ci en version non accentuée.

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

Remarque : la règle de transformation prévaut même si le document présenté comporte une traduction phonétique différente. Par exemple : MŰLER, codé MUELER en bas d'un passeport bulgare, est à enregistrer comme MULER.

4.2.2 *Règles particulières concernant les traits stricts*

Si le jour de la naissance est inconnu, on enregistre par défaut « 01/MM/AAAA ».
Si le mois n'est pas connu, on enregistre par défaut le mois de janvier « JJ/01/AAAA ».
Si le jour et le mois ne sont pas connus, on enregistre par défaut la date du 31 décembre de l'année de naissance : « 31/12/AAAA »
Si l'année n'est pas connue précisément, on enregistre par défaut la décennie :JJ/MM/AAA0

> *Il en résulte que pour une date de naissance inconnue, on enregistre 31/12 et une décennie compatible, par exemple, 31/12/1970 (cf. Instruction générale relative à l'état civil du 2 novembre 2004).*

En présence d'une discordance entre les données d'identité officielles et celles enregistrées par l'assurance maladie, il faut saisir dans les traits stricts les éléments indiqués sur le document d'identité. Les éléments discordants portés par la carte Vitale ne doivent être saisis que s'il existe des champs spécifiques dans le système d'information permettant de préciser ces traits étendus.

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).

4.2.3 *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 naissance (nom de famille, selon la dénomination de l'état civil) et du prénom de naissance, ils ne doivent en aucun cas être saisis dans les traits stricts mais enregistrés dans les traits étendus, charge 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).

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

L'enregistrement des prénoms secondaires doit s'effectuer dans le champ réservé aux 2ème, 3ème, 4ème prénom lorsque le logiciel des structures de santé le prévoit.

Lorsqu'il ne le prévoit pas, l'enregistrement doit s'effectuer dans le champ réservé au prénom, séparés de virgules (exemple : « Prénom1, Prénom2, Prénom3 »).

4.3 Règles d'impression

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

Remarque : cette recommandation ne s'applique pas aux identités sensibles (cf 3.2.4.a) qui font l'objet de procédures spécifiques.

Les données portées sur les étiquettes et documents imprimés par les différents intervenants habilités à le faire (admissions, secrétariat, service de soins, plateau technique…) distinguent bien :

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

Afin d'éviter les ambiguïtés, notamment dans les échanges entre structures différentes, les types de données sont nommés de manière explicite, qu'ils soient présentés de manière complète ou abrégée. La nomenclature ci-dessous peut être proposée :

Traits	Nom du champ explicite	Nom du champ abrégé
Nom de naissance	Nom naissance	N.Nais
Date de naissance	Date naissance	DDN
Genre	Genre	G
Prénom	Prénom	Pr.
Nom d'usage	Nom d'usage	N. Us

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

Une procédure définit les modalités à suivre dans le cas d'une anomalie constatée concernant l'identité d'un usager provenant d'une autre structure afin d'informer la (ou les) structure(s) concernée(s) (cf.4.4).

4.4 Procédures

En fonction de la taille de la structure, de la variété des prises en charge et des risques identifiés, un certain nombre de procédures opérationnelles doit être formalisé et mis en application par toutes les parties prenantes, en application de la charte d'identification.

Les exemples ci-dessous correspondent aux bonnes pratiques recensées dans la région et sont fournis à titre d'illustration. Ils peuvent être amenés à évoluer :

Procédures d'admission :

- Identification primaire à l'accueil de l'usager dans la structure ;
- Identification provisoire de l'usager en situation d'urgence ;
- Enregistrement d'un usager incapable de donner ou justifier son identité ;
- Identification des victimes lors de situation sanitaire exceptionnelle (afflux massif) ;
- Admission d'un usager souhaitant garder l'anonymat ;

Procédures d'identification secondaire :

- Identification secondaire d'un usager avant tout acte de soin ;
- Utilisation du bracelet d'identification ;

Procédures de contrôle et de gestion des bases d'identité :

- Contrôle qualité des bases d'identités ;
- Correction et rapprochement d'identités (et/ou fusion) ;
- Gestion de la diffusion ;
- Gestion des homonymes ;

Procédures en mode dégradé :

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

4.4.1 Modification et rapprochement d'identité

a) Modification d'identité

Le processus de modification d'identité est décrit dans une procédure spécifique. Elle ne peut être mise en œuvre que par les personnels habilités de la structure.

Toute modification s'assoie sur un document d'identité répondant aux critères de la procédure du recueil de l'identité (cf. 3.1). Le système d'information garde une trace de la modification effectuée (historisation, motivations et pièces justificatives) et du niveau de confiance à accorder à l'identité nouvellement saisie

b) Rapprochement dans le domaine d'identification (fusion)

Le processus de fusion de dossier est décrit dans une procédure spécifique. Elle ne peut être mise en œuvre que par les personnels spécialement habilités, sous le contrôle de la cellule d'identito-vigilance (CIV)..

Le système d'information doit garder une trace de la modification effectuée (« historisation », motivations et pièces justificatives).

Après modification ou fusion d'identité, l'information est transmise à tous les acteurs concernés, internes et externes à la structure. Il est également vérifié que l'ensemble des pièces du dossier comporte l'identité mise à jour.

c) Rapprochement dans les logiciels périphériques

La fusion ou la modification d'identités réalisée dans le domaine d'identification est, le cas échéant, appliquée en cascade dans les logiciels non directement interfacés avec le serveur d'identité dans le cadre d'une procédure spécifique. Cette démarche est confiée aux référents des logiciels métiers concernés (cf. 6.1.3).

d) Identification des homonymes

La notion d'homonymie est définie comme la correspondance exacte entre plusieurs traits stricts (description 4.4.1).

La détection d'homonymes doit conduire à identifier formellement ce statut dans la base d'identité pour faciliter la vigilance. Des caractères déterminants doivent être définis pour distinguer les différents homonymes de la base (ex : indexation, ajout des autres prénoms…).

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 tels que : contact téléphonique, alerte par message, étiquetage spécifique.

4.4.2 Identification secondaire

L'identification secondaire vise à reconnaitre et retrouver un usager déjà connu tout au long du processus de prise en charge. Elle va au-delà de la gestion administrative et informatique des identités. Il s'agit d'un axe majeur de formation et de sensibilisation des personnels afin de garantir la sécurité de l'usager et la qualité de sa prise en charge (cf.infra 4.5).

a) Identification de l'usager lors d'un acte de soins

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

- Les questions ouvertes à poser pour vérifier l'identité d'une personne (qui, quand, comment) ;
- L'utilisation pratique de bracelets d'identification.

b) Dispositifs d'identification physique

Plusieurs dispositifs peuvent participer à l'identification des patients tels que la pose d'un bracelet ou l'utilisation d'une photographie dans le dossier patient. L'emploi d'un dispositif d'identification est particulièrement utile pour les usagers :

- Admis pour une hospitalisation (y compris en hospitalisation de jour) ;

- Bénéficiant d'un acte de soins pour lequel une erreur d'identité peut être dommageable ou préjudiciable (biopsie, endoscopie, imagerie interventionnelle, chimiothérapie, traitement allergisant…) ;
- Nouveaux nés ;
- Avec lesquels la communication est difficile : non francophone, patient incapable de parler, confus, inconscient, dément…
- Décédés, non porteurs d'un bracelet au cours de leur séjour, en vue de leur transfert en chambre mortuaire…

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

- L'information de l'usager, de sa famille, sa personne de confiance ou de son représentant légal
- Les modalités de préparation, de pose et dépose du bracelet ou de mise à jour de la photographie ;
- Les modalités pratiques d'utilisation ;
- La conduite à tenir en cas de refus de ce type d'identification ou de nécessité de dépose du bracelet en cours de séjour.

Il faut éviter la transcription manuelle de l'identité de l'usager sur le bracelet (source d'erreurs) et privilégier les bracelets comportant une identité imprimée à partir des données informatisées (cf. 4.3).

c) *Identification des documents du dossier de l'usager*

Les structures de santé doivent veiller à ce que tous les documents liés à la prise en charge d'un usager (courrier, feuille de surveillance, document de transfert…) soient identifiés sur toutes les pages par, au minimum, les traits stricts (cf. 3.2).

De même, il doit exister une procédure qui précise les modalités pratiques de numérisation et d'identification des documents numérisés joints au dossier informatique de l'usager afin de limiter le risque d'erreur d'attribution. Une procédure doit également préciser les modalités de modification de documents scannés ou d'images qui comportent une identité erronée.

4.5 Formation et sensibilisation à l'identitovigilance

4.5.1 *Formation du personnel*

La structure doit prévoir des actions de formation et de sensibilisation à l'ensemble des personnels concernés par la mise en œuvre des règles d'identitovigilance. Elles prennent en compte tous les aspects de l'identitovigilance et concernent aussi les intervenants externes (ambulanciers, professionnels et structures adressant des usagers, plateaux techniques…) et temporaires (stagiaires et intérimaires notamment).

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

4.5.2 *Sensibilisation des usagers*

Les établissements respectent le Règlement général sur la protection des données (RGPD) et les principes des chartes relatives aux droits des usagers s'appliquant dans leurs structures (charte de la personne hospitalisée, charte de l'usager en santé mentale, charte de la personne accueillie).

Dans le cadre de l'identitovigilance, une attention particulière est portée aux droits :

- 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 vigilance doit être portée à la communication réalisée auprès des usagers et des accompagnants (affichage, livret d'accueil…), afin de :

- Leur permettre de comprendre l'importance de l'Identitovigilance, pour leur propre sécurité.
- De les inciter à participer à leur identification et à vérifier les informations utilisées pour les identifier.

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

5. Indicateurs qualité

Les indicateurs qualité ont pour but d'évaluer la performance du système. La charte régionale retient les indicateurs suivants :

Indicateurs concernant le suivi de la qualité du processus de l'identification :

- Nombre total de dossiers actifs, à l'exclusion des dossiers archivés

Définition des dossiers actifs : une venue réactivée dans les 5 ans depuis 2014. Cette notion peut être modulable en fonction du champ d'activité (notamment dans le cadre de la prise en charge psychiatrique ambulatoire)

- Nombre total de nouveaux patients créés par année
- Nombre total d'identité patient « Provisoire »
- Nombre total d'identité patient « validée »
- Taux de rapprochement d'identité (sous réserves de capacité à produire cette indicateur)
- Nombre d'identités « provisoires » qui sont passées « validées » sur le nombre d'identités créées à l'année
- Nombre d'usurpations d'identité détectées (sous réserves de capacité à produire cette indicateur)

Indicateurs concernant le suivi des aspects organisationnels :

- Nombre de formations organisées par an (volume horaire)
- Nombre d'agents formés par an/ effectif de l'établissement

Indicateurs concernant le suivi des anomalies :

- Nombre de doublons
- Nombre de collisions
- Nombre de fusions
- Nombre de dé-fusions

6. Sécurité

6.1 Sécurité du système d'information

La politique de sécurité du système d'information des établissements prend en compte le règlement général sur la protection des données (RGPD)

6.1.1 *Droits de création et modification d'identité*

Les droits de création et de modification d'identité dans le système d'information doivent être réservés à un nombre limité de professionnels. Ils sont nommément désignés par le responsable de la structure, en cohérence avec la politique d'habilitation des personnes autorisées à créer ou valider l'identité d'un usager : bureau des entrées, urgences, secrétariat médical….

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

6.1.2 *Procédures*

Une charte informatique formalisant les règles d'accès et d'usage du système d'information, 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.

6.1.3 *Droits de rapprochement et fusion*

La possibilité de faire une fusion ne doit être attribuée qu'à des membres spécialement désignés de la CIV. Les droits individuels doivent être tracés dans un document qualité adapté (cf. 4.4).

La structure de santé prend les dispositions nécessaires pour organiser la réalisation des fusions dans les logiciels tiers lorsque la fusion n'est pas intégrée automatiquement (cf. 6.1.5).

Les opérations doivent être tracées.

6.1.4 *Confidentialité*

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

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

Excepté dans les cas de dérogation expressément prévus par la loi, un professionnel accède au dossier numérique (réseau et logiciels) ou physique (papier) d'un usager uniquement s'il contribue à assurer

sa prise en charge, et ce dans le respect du droit au respect de la vie privée et au secret des informations concernant l'usager (Art L1140-4 CSP)

Les accès aux données de santé numériques par les professionnels doivent être enregistrés et horodatés. Des précautions particulières doivent être prévues lorsqu'un professionnel accède aux données de patients dont il n'assure pas directement la prise en charge.

6.1.5 *Référents logiciels*

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

6.2 Respect du cadre d'interopérabilité des systèmes d'information en santé (CI-SIS)

La démarche d'identitovigilance et les outils mis à son service s'inscrivent dans le cadre d'interopérabilité des systèmes d'information en santé et du RGPD.

Il est essentiel de garantir la conformité au cadre juridique et légal des systèmes d'information. Dans ce contexte, la structure veille à l'information des usagers et au respect de leurs droits.

6.2.1 *Le référentiel unique d'identités*

La structure doit disposer d'une solution de gestion des identités, ensemble de composants techniques et organisationnels, qui garantit la cohérence des données d'identités pour toutes les applications.utilisées par les professionnels de santé et du médico-social lors de la prise en charge ou du suivi des personnes.

Ce référentiel unique devra être capable :

- d'échanger avec la future solution régionale d'identification,

- de gérer l'INS, identifiant national de santé, qui est constitué du NIR, numéro d'inscription au RNIPP (répertoire national d'identification des personnes physiques -Article L 1111-8-1 du CSP) pour la prise en charge des personnes à des fins sanitaires ou médico-sociales.

6.2.2 *Analyse des impacts de la charte sur les fonctions du systèmed'information*

La charte régionale d'identification de l'usager dans son parcours de santé et sa déclinaison locale dans les structures peuvent avoir un impact sur le système d'information et l'organisation de celles-ci. Il est donc recommandé de mettre en place un audit ou une étude d'impact sur les processus internes

(processus d'admission, de production de soins, de pilotage et de facturation et de support…) et externes (télémédecine, EFS, …), et sur le système d'information (analyse d'impact, en se basant sur la cartographie des applications et des flux d'échanges…). L'étude d'impact définira le plan d'action à mettre en œuvre, ainsi que le planning et le budget à prévoir.

Pour cela, la structure définira les niveaux d'autorisation par catégorie professionnelle, par catégorie de données ou par fonctions.

Le RGS (référentiel général de sécurité) constitue également un cadre de référence impératif. Il impose lors d'une transmission électronique entre le patient et la structure, ou entre structures, la retranscription d'un compte rendu des informations télétransmises (principe de l'accusé réception des informations et mise en œuvre d'une analyse des risques du processus).

Les données démographiques du patient sont des données à caractère personnel qui nécessitent donc un niveau de sécurité assurant notamment la confidentialité des données.

Outre les précautions élémentaires à mettre en œuvre dans la structure de santé (accès physique et logique aux serveurs et ordinateurs, mots de passe …), la structure devra mettre en place une gestion des droits d'accès aux données démographiques du patient et en assurer la traçabilité.

6.2.3 *Cartographie des risques*

L'analyse a priori des risques est une méthode d'analyse systémique des risques tout au long des étapes d'un processus. La structure mettra en place une analyse a priori des risques lorsqu'elle décrira son processus d'identification et élaborera ses procédures. Les risques sont hiérarchisés selon leur criticité (fréquence, gravité, détectabilité).

Les instances régionales interviendront en soutien des structures locales pour mettre en place une cartographie des risques commune.

7. Glossaire

1.1.1.1.1. 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.

1.1.1.1.2. 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.

1.1.1.1.3. 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.

1.1.1.1.4. 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.

1.1.1.1.5. 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.

1.1.1.1.6. 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.

1.1.1.1.7. Fusion

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

1.1.1.1.8. Homonymie

La notion d'homonymie est définie comme la correspondance exacte entre plusieurs traits stricts (cf.4.4.1).

1.1.1.1.9. 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)…

1.1.1.1.10. Identifiant national de santé (INS) (ex NIR)[1]

L'utilisation de l'identifiant national de santé (INS) est un critère de la bonne qualité d'identification du patient nécessaire à la confiance dans les services numériques.

L'INS est une donnée personnelle, protégée par la CNIL (Commission Nationale des informations et Libertés). Il est donc unique, univoque, pérenne et reconnu par tous les acteurs de santé. La loi consacre le NIR (numéro d'inscription au répertoire national d'identification des personnes physiques, plus communément appelé « numéro de sécurité sociale ») – à défaut le NIA (numéro identifiant attente) - comme INS, en remplacement de l'INS-C (INS calculé) précédemment utilisé comme identifiant national. La mise en œuvre démarre en 2019. En attendant, l'INS-C peut être utilisé comme identifiant.

1.1.1.1.11. 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…).

[1] Référentiel du 24 décembre 2019 relatif à l'identifiant national de santé : https://esante.gouv.fr/sites/default/files/media_entity/documents/ASIP_R%C3%A9f%C3%A9rentiel_Identifiant_National_de_Sant%C3%A9_v1.pdf

1.1.1.1.12. 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.

1.1.1.1.13. Interopérabilité de systèmes informatiques

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

1.1.1.1.14. 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 le 24 décembre 2019, en définit les modalités de mise en œuvre, dispensant alors les utilisateurs habilités à déclarer son utilisation auprès de la CNIL (Décret n°2019-1036 du 8 octobre 2019 modifiant le Décret n° 2017-412 du 27 mars 2017)

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 (genre, année et mois de naissance, département et commune de naissance, numéro d'ordre du registre d'état civil) ;
- Soit par la CNAV lors de l'inscription sur le système national de gestion des identités (SNGI) à la demande d'un organisme de sécurité sociale (tels que CARSAT, CPAM, CAF, MSA, RSI), 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 CNAV 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 CNAV au plus tard le 31 décembre 2018. Les professionnels habilités pourront y accéder à partir de la carte Vitale ou, lorsque cette information n'est pas disponible, au moyen des services de recherche et de vérification de l'identifiant de santé mis en œuvre par la CNAMTS.

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

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

1.1.1.1.15. Nom de naissance (nom de famille, selon la dénomination de l'état civil)

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 nom de naissance est retenu au périmètre de la région comme le nom de famille (y compris pour les femmes mariées). Le nom marital étant considéré comme le nom d'usage.

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.

1.1.1.1.16. Nom d'usage

Toute personne possède un nom de naissance. Il est néanmoins possible d'utiliser, dans la vie quotidienne, un autre nom appelé nom d'usage. Ce nom d'usage ne remplace en aucun cas le nomde naissance qui reste le seul nom mentionné sur les actes d'état civil.

Sur la carte d'identité, il est précisé sous la rubrique « Nom » après « Nom d'usage », « Époux(se) » ou « Veuf(ve) ».

1.1.1.1.17. Prénom de naissance

L'attribution d'un prénom est obligatoire : il est indiqué sur l'acte de naissance. Lorsqu'il encomporte plusieurs, c'est le premier prénom qui sert de prénom de naissance : il est celui qui apparaît avant la virgule sur la carte d'identité (cf. 3.2).

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

1.1.1.1.18. Prénom d'usage (Alias du prénom)

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

En termes d'identitovigilance, il ne remplace pas le premier prénom du document d'identité (cf. 3.1) et ne peut être enregistré que dans les systèmes d'information qui dispose d'un champ spécifique (cf. 3.1).

1.1.1.1.19. Pseudonyme (alias nom et/ou prénom)

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

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

Ex : « Dit : Johnny Hallyday »

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

1.1.1.1.20. 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…

1.1.1.1.21. Surnom

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 ».

1.1.1.1.22. 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.

ANNEXE 1 – Références réglementaires et techniques

- Article R1112-3 du Code de la Santé Publique
- Article L162-21 du Code de la Sécurité sociale
- Loi n° 2002-304 du 4 mars 2002 relative au nom de famille
- Instruction générale relative à l'état civil du 2 novembre 2004
- Circulaire du 28 juin 1986 relative à la mise en œuvre de l'article 43 de la loi n° 65-1372 du 23 décembre 1985. Usage du nom du parent qui n'est pas transmis. Dénomination des personnes dans les documents administratifs.
- Circulaire du 28 octobre 2011 relative aux règles particulières à divers actes de l'état civil
  relatifs à la naissance et à la filiation
- Instruction N° DGOS/MSIOS/2013/281 du 7 juin 2013 relative à l'utilisation du nom de famille (ou nom de naissance) pour l'identification des patients dans les systèmes d'information des structures de soins.
- Circulaire n° INT/D/00/00001/C du 10 janvier 2009 relative à l'établissement et la délivrance des cartes nationales d'identité.
- La loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle - Guide méthodologique Mise en œuvre de l'identité patient au sein des groupements hospitaliers de territoire (ASIP Santé, 2018)
- Décret n° 2016-46 du 26 janvier 2016 relatif à la biologie médicale
- Arrêté du 15 mai 2018 fixant les conditions de réalisation des examens de biologie médicale d'immuno-hématologie érythrocytaire
- Décret n°2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé
- Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
- Arrêté du 24 décembre 2019 portant approbation du référentiel « Identifiant National de Santé »