pulsy

Groupement Régional d'Appui
au Développement de la e-santé
–
GRAND EST

CHARTE REGIONALE DI'IDENTITOVIGILANCE

pulsy

HISTORIQUE DES RÉVISIONS

Date	Version	Description	Auteur
05/04/2022	0.0	Rédaction, Relecture et Modifications par le groupe de travail	Groupe de travail régional

TABLE DES MATIÈRES

1 INTRODUCTION

La charte régionale a été construite en se basant sur des chartes régionales déjà existantes et sur le retour d'expérience des membres du groupe de travail.

La version finale, validée par le comité consultatif régional d'identitovigilance Grand Est, tient compte du référentiel INS, de la doctrine technique du numérique en santé et est conforme avec les bonnes pratiques décrites dans le Référentiel national d'identitovigilance (RNIV).

1.1 Contextes et enjeux

La bonne identification des usagers est un facteur essentiel pour garantir la qualité et la sécurité de leur prise en charge tout au long de leur parcours de soins.

L'identitovigilance représente l'ensemble des moyens organisationnels et techniques mis en œuvre pour disposer d'une identification unique, fiable et partagée de l'usager afin d'éviter les risques d'erreurs tout au long de son parcours de santé.

Les règles d'identitovigilance définies par le Référentiel National d'identitovigilance (RNIV) s'imposent à l'ensemble des usagers du système de santé, qu'ils soient professionnels médicaux, paramédicaux, administratifs, ou patients.

Elles sont un prérequis pour la sécurisation du partage d'informations de santé, qu'il soit réalisé au sein de la structure ou lors des échanges avec les référents médicaux de l'usager, dans le respect du secret médical.

Le développement des échanges d'informations, le partage de données médicales entre professionnels de santé, s'imposent pour développer la télémédecine et la télésanté, des pratiques coordonnées, les parcours de soins et parcours de santé.

Une identité consolidée est un élément stratégique de ce développement, c'est la raison pour laquelle l'utilisation de l'Identité Nationale de Santé (INS) pour référencer les données de santé est obligatoire depuis le 1er janvier 2021.

1.2 Objectifs de la charte

La charte régionale d'identitovigilance du Grand-Est poursuit les objectifs suivants :
- Définir la politique d'identification du patient afin d'améliorer la qualité des prises en charge dans le cadre de la continuité, des parcours de soins et du partage d'information et limiter les risques d'erreur d'identification.

- Favoriser le respect des bonnes pratiques d'identification des usagers par les professionnels.
- 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 parcours de santé commun.
- Garantir la confiance dans la qualité des informations échangées entre les systèmes d'informations et les professionnels de santé.
- Permettre une communication commune et partagée en matière d'identitovigilance.
- Sécuriser le rapprochement.
- Contribuer à l'interopérabilité des systèmes d'information de santé.

1.3 Périmètre d'application

Dans une perspective d'harmonisation durable des pratiques, la politique régionale d'identitovigilance s'applique à tous les modes de prise en charge du patient et d'accueil dans les secteurs sanitaire et médico-social.

Sont concernés par cette pratique :

- Les usagers, acteurs de leur sécurité (y compris les ayants-droits et les personnes de confiance)
- Les professionnels qui interviennent sur les données médico-socio-administratives des usagers
- Les acteurs de santé assurant la prise en charge.

Cette charte doit être bâtie par consensus avec les professionnels de santé de la région Grand-Est et ensuite se décliner localement dans chacune des structures de santé.

2 POLITIQUE D'IDENTITOVIGILANCE

2.1 Gouvernance

La charte régionale d'identitovigilance s'adresse à toutes les structures sanitaires et médicosociales, aux réseaux de soins et aux professionnels de santé libéraux intervenant dans la région Grand-Est.

Par la suite, le terme utilisé pour nommer ces différentes organisations sera le terme structures de santé.

2.1.1 Gouvernance régionale

- Le comité consultatif régional d'identitovigilance (CCRIV)

> Missions :

- Définir la politique régionale d'identification des patients, en conformité avec la politique nationale et les exigences des différents volets du RNIV ;
- Suivre les indicateurs et les évaluations relatifs à l'identification des usagers de la santé
- Alerter sur les situations à risque et éclairer l'ARS et le GRADeS sur les orientations stratégiques
- Contribuer à la réalisation et à l'évaluation des actions en lien avec la CRIV. Notamment, le CCRIV pourra aider à :
    - Assurer la veille réglementaire ;
    - Valider la pertinence et la priorité des actions à conduire ;
    - Evaluer l'impact et la faisabilité des décisions ;
    - Mettre en place des groupes de travail pour produire des outils pratiques ou répondre à des problématiques particulières ;
    - Participer à la diffusion et la promotion des bonnes pratiques…

- Composition :
  - Référents en identitovigilance exerçant dans une structure de santé ;
  - Responsables de traitement des solutions informatiques ;
  - Représentants des parties prenantes (professionnels de santé, médico-sociaux, usagers, développeurs informatiques, sous-traitants, responsables de systèmes d'information…) reconnus pour leur expertise sur la thématique.

  D'autre professionnels pourront être conviés selon les thématiques traités, et notamment dans le cadre des groupes de travail.

- Fonctionnement :
  Les membres du CRCIV désignent en leur sein un président de comité, chargé du bon fonctionnement du CRCIV. Sa désignation est renouvelée a minima une fois par an, selon des modalités définies dans une charte de fonctionnement de l'instance.
  La CRCIV se réunit au moins 3 fois par an. L'ordre du jour est transmis au moins 8 jours avant la réunion. Chaque réunion donne lieu à la rédaction d'un relevé de décision et d'action

  En tant que de besoin, la CRCIV pourra décider de constituer des groupes de travail, dédiés aux problématiques à traiter, et de composition adaptée aux thématiques traitées.

- La cellule régionale en identitovigilance (CRIV)
- Missions :
  - Mettre en œuvre la politique d'identitovigilance définie par le CRPIV ;
  - Constituer et animer un réseau régional de référents d'identitovigilance ;
  - Former et accompagner les professionnels de santé dans le respect et la mise en œuvre des recommandations de bonnes pratiques nationales et régionales ;
  - S'assurer de l'application des bonnes pratiques ;
  - Promouvoir la déclaration des événements indésirables liés à des erreurs d'identification ;
  - Participer aux retours d'expériences et à la communication régionale en retour ;
  - Organiser la conduite d'actions préventives et correctives, au niveau régional ;
  - Réaliser la veille règlementaire et documentaire ;
  - Tenir à jour la base documentaire régionale ;
  - Effectuer le suivi et l'analyse des indicateurs régionaux.

- Composition :

La CRIV regroupe des personnels dédiés et identifiés pour leurs connaissances et leurs compétences en identitovigilance. Ses effectifs sont adaptés aux besoins et missions confiés par le CRPIV.

La CRIV est rattaché au GRADeS de la région.

- Fonctionnement :

Le fonctionnement de cette instance est, par définition, continu.

- Le référent régional en identitovigilance

  Le référent régional en identitovigilance est un professionnel désigné par l'ARS pour ses compétences en identitovigilance. Membre de droit des différentes instances de gouvernance régionale, il est l'interlocuteur privilégié pour tout ce qui concerne l'identification primaire ou secondaire du patient :

- De l'ARS
- Du réseau régional de vigilances et d'appui (RREVA) ;
- De la structure régional d'appui à la qualité et la sécurité des soins (SRA) ;
- Du groupement régional d'appui au développement de la e-santé (GRADeS) ;
- Des autres référents régionaux, au sein du réseau des référents régionaux en identitovigilance (3RIV).

  Le référent régional en identitovigilance est placé pour emploi auprès du GRADeS.

2.1.2 Au niveau local

A partir de la charte régionale d'identitovigilance, les structures de santé du Grand-Est peuvent élaborer leur propre charte en reprenant les principes obligatoires, ou mettre à jour une charte existante afin de converger vers une identification partagée du patient au niveau régional.

Pour assurer une bonne application de la politique de l'identitovigilance au sein des structures de santé, elles doivent mettre en place une ou plusieurs instances de gouvernance adaptée (s) à leur taille et à leur activité.
On distinguera :

- Une instance stratégique qui décidera de la politique à mener en matière d'identitovigilance et les moyens fournis pour y parvenir ;
- Une instance opérationnelle qui appliquera et évaluera les procédures en vigueur.

2.2 Référentiel INS

Différentes obligations découlant du RGPD et la Loi relative à l'informatique aux fichiers et aux libertés (LIL) de 1978 sont formulées dans le référentiel INS (voir Annexe Régime juridique applicable au référencement des données avec l'INS):

- Respecter l'obligation de référencer les données avec l'INS
- Respecter la liste des données concernées par l'opération de référencement
- Transmettre les données référencées avec l'INS uniquement aux acteurs légitimes à en être destinataires
- Respecter la durée de conservation des données

3 DEFINITIONS ET TERMINOLOGIE

3.1 Identité et identifiants numériques

3.1.1 Identité

Ensemble de données, ou traits d'identité, qui constituent la représentation d'une personne physique.

3.1.2 Identité numérique

L'identité numérique correspond à la représentation d'un individu physique dans un système d'information.
Un même usager peut avoir plusieurs identités numériques : dans le (ou les) domaines d'identification ou de rapprochement utilisés par la structure, dans son dossier médical partagé (DMP), dans la base de données de facturation de l'assurance maladie.

3.1.3 Identifiant numérique

Séquence de caractères qu'un ou plusieurs domaines d'identification utilisent pour représenter une personne et lui associer des informations dans le cadre de sa prise en charge (ex : IPP)

3.1.4 Identité Nationale de Santé (INS)

C'est une identité numérique unique, univoque, pérenne, permettant de référencer, de conserver et de transmettre les informations de santé d'un usager. Son utilisation est obligatoire à compter du 01/01/2021 par l'ensemble des professionnels de santé. Elle correspond aujourd'hui à l'identité INS.

Ensemble des informations numériques renvoyés par le téléservice INSi, constituées :

- du matricule INS : numéro d'identification au répertoire des personnes physiques (NIR ou NIA) ;

- des traits INS (Nom de naissance, liste des prénoms de l'état civil, date de naissance, sexe, code commune du lieu de naissance ou code pays pour les personnes nées à l'étranger) ;

- de l'OID (object identifier) qui identifie l'origine et le type de l'information (INSEE, NIR/NIA…).

L'INS est une donnée personnelle, protégée par la CNIL.

3.1.5 NIR

Le numéro d'inscription au répertoire des personnes physiques (NIRPP ou NIR) sert à identifier une personne dans le répertoire national d'identification des personnes physiques géré par l'INSEE (RNIPP).

Le NIR personnel constitue le matricule 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).

Le NIR est attribué :

- soit par l'INSEE lors de l'inscription au RNIPP ; l'inscription a lieu, en général, au plus tard huit jours après la naissance, à partir de l'état civil transmis par les mairies (sexe, année et mois de naissance, département et commune de naissance, numéro d'ordre du registre d'état civil) ;

- soit par la CNAV lors de l'inscription sur le système national de gestion des identités (SNGI) à la demande d'un organisme de sécurité sociale, à l'occasion d'une démarche effectuée par la personne elle-même ou par son employeur.

3.1.6 NIA

C'est le numéro d'immatriculation d'attente (NIA) attribué par la CNAV aux personnes nées à l'étranger 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 et qu'aucun doublon n'est possible avec un autre NIR. En l'absence de NIR, le NIA constitue le matricule 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).

3.1.7 Matricule INS

Identifiant de l'identité INS, représenté par le NIR ou le NIA personnel de l'usager.

3.2 Domaines d'identification et de rapprochement

3.2.1 Domaine d'identification

Il regroupe au sein d'une organisation de santé toutes les applications qui utilisent le même identifiant pour désigner un patient.

Exemples :

- un cabinet médical disposant d'un mode unique d'identification de ses patients est considéré comme un domaine d'identification ;

- un établissement de santé dont tous les logiciels utilisent le même identifiant est un domaine d'identification.

3.2.2 Domaine de rapprochement

Il rassemble au moins deux domaines d'identification qui échangent ou partagent des informations entre eux. On distingue les domaines de rapprochements intra établissement et extra établissement.

Exemples :

- un établissement de santé disposant d'un Identifiant Permanent du Patient (IPP) et dont une partie des logiciels utilise un identifiant et une autre partie des logiciels un autre identifiant est un domaine de rapprochement. En effet, dans cet exemple, il existe deux groupes de logiciels et chaque groupe utilise un identifiant qui lui est propre. Chaque groupe constitue donc un domaine d'identification différent. L'établissement dispose également d'un IPP qui lui permet d'échanger des informations entre les deux domaines d'identification. Ce domaine de rapprochement est un domaine de rapprochement intra établissement ;

- si des établissements de santé alimentent un serveur régional d'identité et de rapprochement, alors ce serveur constitue un domaine de rapprochement.

3.3 Vocabulaire de l'identitovigilance

Le vocabulaire couramment employé en identitovigilance est défini dans l'annexe II du volet RNIV 1.

3.3.1 Collision

C'est une anomalie correspondant au référencement avec une même identité de données concernant 2 personnes physiques différentes, ou plus, notamment dans les cas suivants : sélection erronée d'un dossier informatique, usurpation d'identité d'un tiers déjà enregistré, erreur d'opération de fusion entre dossiers n'appartenant pas au même usager… 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.

3.3.2 Dé-fusion

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.

3.3.3 Doublon (d'identités)

On parle de doublons (ou de n-uplet) d'identités lorsqu'une même personne est enregistrée sous 2 identifiants différents (ou plus) dans un même domaine d'identification. 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.

3.3.4 Fusion

Elle correspond au transfert, sur un identifiant unique, de toutes les informations concernant le même usager dispersées sur plusieurs identifiants (doublons) d'un même domaine d'identification.

3.3.5 Rapprochement d'identités

Attribution d'une identité numérique (dite identité de fédération) commune à plusieurs identités numériques appartenant à des domaines d'identification différents (au niveau territorial, régional) mais qui font référence au même usager.

4 L'IDENTIFICATION DU PATIENT

L'identification du patient est l'opération visant à attribuer de manière univoque à l'usager une identité qui lui est propre grâce au recueil de différents traits. Dans un système d'information elle consiste au rattachement à un identifiant existant ou à la création d'un nouvel identifiant.

4.1 Identification primaire et identification secondaire

4.1.1 Identification primaire

C'est l'ensemble des opérations destinées à attribuer de manière univoque à une personne physique une identité numérique qui lui est propre. L'identification primaire comprend les étapes de recherche d'un patient dans la base, de création ou de modification d'une identité, de validation de cette identité, de récupération de l'identité INS via l'appel au téléservice INSi.

4.1.2 Identification secondaire

Elle correspond à la vérification, par tout professionnel de santé, de l'identité de l'usager physique tout au long de sa prise en charge avant la réalisation d'un acte le concernant (prélèvement, soins, transport, acte technique…). Elle comprend également l'identification des prélèvements ou des documents de l'usager et la sélection du bon dossier dans une application utilisée au sein d'un service de soins (prescription, dossier de soins, résultats d'examens…).

4.2 Données démographiques du patient

4.2.1 Les traits stricts

Les traits stricts définis par le RNIV :

- Le nom de naissance ;
- Le premier prénom d'état civil ;
- Liste des prénoms de naissance figurant sur un titre officiel d'identité ;
- La date de naissance ;
- Le code INSEE du lieu de naissance ;
- Le sexe ;
- Le matricule INS (associé à son OID afin de le distinguer du NIR ou du NIA)

Ces traits sont des informations de référence peu variables dans le temps et facilement accessibles depuis une pièce d'identité à haut niveau de confiance.

Ils sont indispensables à la recherche et l'identification d'un patient, ils permettent de référencer les données de santé partagées et de fiabiliser les rapprochements d'identités numériques entre structures.

4.2.2 Les traits complémentaires

Les traits étendus sont :

- Le nom d'usage ;
- L'adresse ;
- Le numéro de téléphone fixe
- Le numéro de téléphone portable ;
- L'adresse e-mail ;
- Les numéros INS-C et INS ;
- La situation familiale.

Ces traits sont utilisés en complément des traits stricts pour l'identification du patient.

5 RECUEIL DE L'IDENTITE PATIENT

Le recueil d'identité comprend la création, la recherche et la modification des identités patients.

La vérification de la cohérence des informations concernant l'identité d'un individu avec une pièce d'identité à haut niveau de confiance est obligatoire pour considérer cette identité comme valide.

5.1 Accueil du patient

L'identification primaire débute dès l'accueil du patient, par le biais d'une question ouverte et la consultation d'une pièce d'identité afin de dépister les erreurs et les éventuelles usurpations d'identité.

5.2 Création d'une identité

5.2.1 Recherche d'une identité dans la base de données

Afin d'éviter la création de doublons et la survenue de collisions la recherche d'antériorité est obligatoire.
A chaque fois que cela est possible l'agent doit demander au patient s'il est déjà venu dans la structure de santé.

La recherche de l'enregistrement d'un usager est impérative avant toute création d'une nouvelle identité et doit être réalisée ainsi :

- La recherche s'effectue obligatoirement sur la date de naissance, puis est affinée sur les autres traits stricts ;
- La recherche ne doit jamais se faire sur l'identité complète (nom, prénom, date de naissance) mais sur les premières lettres du nom et du prénom de naissance ;
- Les noms d'usage doivent également être recherchés le cas échéant.
- La recherche peut être effectuée à partir de tout ou partie de l'identité INS récupérée après l'interrogation du téléservice INSi

L'utilisation du matricule INS pour la recherche d'antériorité doit être sécurisée pour éviter tout risque lié à une erreur de saisie. Si le matricule n'est pas récupéré électroniquement, la saisie des 15 caractères du NIR et leur validation par la clé de contrôle est obligatoire pour toute recherche à partir du matricule INS.

5.2.2 Les règles de saisie

Les règles suivantes sont applicables à tous les domaines d'identification de la structure de santé et sont en conformité avec le RNIV.

Les données démographiques doivent être recueillies à partir de documents à haut niveau de confiance, les données enregistrées sur la carte Vitale ne suffisent pas à qualifier l'identité du patient.

- Les noms et prénoms

Doivent être transcrits en caractères majuscules non accentués, sans signe diacritique et sans abréviation, même s'il s'agit d'une suite de « X » ou tout autre mention pour signifier que la personne n'a pas de nom.

Les tirets et apostrophes doivent être conservés, en revanche, les autres caractères tels que « / » doivent être remplacés par un espace.

L'enregistrement du nom utilisé est obligatoire lorsqu'il est différent du nom de naissance.

L'enregistrement du prénom utilisé est obligatoire lorsqu'il est différent du premier prénom de naissance.

- La date de naissance

Lorsque la date de naissance fournie par le document d'identité ou le dispositif d'identification numérique est incomplète, il faut appliquer les consignes suivantes :

- si seul le jour est inconnu, il est remplacé par le premier jour du mois (01/MM/AAAA) ;

- si seul le mois n'est pas connu, il est remplacé par le premier mois de l'année (JJ/01/AAAA) ;

si le jour ET le mois ne sont pas connus, il faut saisir la date du 31 décembre de l'année de naissance26 (31/12/AAAA) ;

- si l'année n'est pas connue précisément, on utilise l'année ou la décennie estimée ;

- si la date de naissance est inconnue, on enregistre 31/12 et une année ou décennie compatible avec l'âge annoncé ou estimé, par exemple, 31/12/1970.

6 QUALIFICATION DE L'IDENTITE PATIENT

6.1 Les statuts de confiance de l'identité numérique

L'attribution d'un niveau de confiance à toute identité numérique est obligatoire.

Le niveau de confiance repose sur deux principes cumulatifs :

- La récupération ou la vérification de l'identité INS par appel au téléservice INSi
- La validation des traits stricts par le biais d'un contrôle de cohérence réalisé à partir d'un dispositif à haut niveau de confiance.

Quatre niveaux de confiance sont ainsi distingués :

- le statut **Identité provisoire** est attribué à toute identité numérique créée sans utilisation du téléservice INSi et sans contrôle de cohérence des traits au moyen d'un dispositif d'i d'identification à haut niveau de confiance ;
- le statut **Identité récupérée** est attribué lorsque l'identité numérique est créée à partir de l'identité INS récupérée après interrogation du téléservice INSi ;
- 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 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 à haut niveau de confiance.

6.2 Les dispositifs d'identité à haut niveau de confiance

Seul un document avec un fort niveau de confiance peut être utilisé pour qualifier l'identité, les autres documents d'identification permettent de créer une identité mais ne sont ni validant ni qualifiant.
Les pièces permettant le recueil de l'identité sont listées dans le tableau ci-dessous.

Libellé	Niveau de confiance
Carte Nationale d'Identité	Forte
Passeport	Forte
Titre permanent de séjour	Forte
Extrait d'acte de naissance pour un enfant né en France (accompagné d'un titre à haut niveau de confiance d'un parent)	Forte
Livret de famille pour les mineurs (accompagné d'un titre à haut niveau de confiance d'un parent)	Forte
Permis de conduire	Moyen
Livret de famille	Moyen
Carte Vitale + Photo	Moyen

En cas de divergence entre deux titres d'identité à haut niveau de confiance, le passeport si présenté est à privilégier.
Dans les autres cas, il convient de prendre en compte les données du document le plus récent.

6.3 L'appel au téléservice INSi

L'Identité Nationale de Santé est recherchée, récupérée et/ou vérifiée par appel au téléservice INSi.

L'interrogation du téléservice est possible :

- par saisie des traits de l'identité numérique locale : nom de naissance, un des prénoms de naissance, sexe et date de naissance.
- par l'intermédiaire de la carte Vitale

Le téléservice INSi renvoie différentes informations contenues dans l'Identité Nationale de Santé et permettant d'identifier l'usager :

- Le matricule INS
- Les traits INS provenant de la base nationale de référence (SNGI) :
    - Le nom de naissance
    - Le(s) prénom(s) de naissance
    - La date de naissance
    - Le sexe

6.4 Point d'attention sur la conservation des données

L'article 5 du 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 CNIL reconnait le caractère légitime de l'enregistrement d'une pièce d'identité dans le cadre de la vérification d'identité. Elle autorise la conservation d'une copie papier dans les mêmes conditions que le dossier médical pour une durée de cinq ans à compter de la dernière venue du patient dans la structure de santé, la conservation des pièces d'identité numériques sous forme chiffrée, et l'accès à cette copie aux professionnels spécifiquement habilités en charge du traitement des anomalies liées à l'identité sous condition de traçabilité et d'historisation des consultations. Le stockage du numéro de la pièce est interdit.

7 UTILISATION DE SERVICES D'E-SANTÉ RÉGIONAUX (SI APPLICABLE)

En cours de rédaction

8 SECURITE DES DONNEES

8.1 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.

8.2 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.

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

Les opérations doivent être tracées.

8.3 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.

8.4 Référents logiciels

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

9 GESTION DES EVENEMENTS INDESIRABLES

En cours de rédaction

10 INDICATEURS

En cours de rédaction

11 RESPECT DU CADRE D'INTEROPERABILITE DES SYSTEMES D'INFORMATION EN SANTE

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.

11.1 Le référentiel unique d'identités

Chaque structure de santé 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 de gérer l'INS.

11.2 Analyse des impacts de la charte sur les fonctions du système d'information

La charte régionale d'identitovigilance 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.

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.

12 FORMATION ET SENSIBILISATION

12.1 Formation du personnel

La formation et la sensibilisation de l'ensemble des personnels concernés par la mise en œuvre des règles l'identitovigilance doivent être prévues par la structure de santé.

Elles prennent en compte tous les aspects de l'identitovigilance et concernent également les intervenants et plateaux techniques externes (ambulanciers, professionnels et structures adressant des patients, …) et temporaires (stagiaires et intérimaires notamment).

Ponctuellement des audits à l'initiative du pilote identitovigilance de la structure de santé peuvent être réalisés afin d'évaluer le bon respect des procédures mises en place et si besoin programmer des nouvelles actions de formations et de sensibilisation.

La cellule locale d'identitovigilance transmettra annuellement à la cellule régionale d'identitovigilance les indicateurs suivants :

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

12.2 Sensibilisation des usagers

Les structures de santé respectent le 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).

L'usager doit être acteur de sa bonne identification tout au long de son parcours de soins et d'accompagnement pour cela l'accent doit être mis sur la communication afin de :

- Lui permettre de comprendre l'importance de l'identitovigilance pour sa propre sécurité.
- L'inciter à participer à son identification et à vérifier les informations utilisées pour les identifier.

Cette sensibilisation passe par un affichage dans les lieux stratégiques : accueils, secrétariats médicaux, admissions, ainsi que la délivrance d'informations dans le livret d'accueil.
Les informations relatives à l'identitovigilance doivent également être diffusées sur le site internet et/ou prise de rendez-vous de la structure.

Les usagers doivent être informés au plus tôt des documents (document d'identité à haut niveau de confiance) qui leur seront réclamés durant leurs prises en charge et de la nécessité des mesures de vérification à chaque étape de leurs parcours de soins.

13 PROCEDURES

En cours de rédaction

14 REFERENCES

- Norme AFNOR : Informatique de santé – Identification du patient dans le processus de soins. Réf. BP S97-723 Décembre 2002
- Etude du GMSIH sur l'identification patient : http://www.anap.fr/publications-et-outils/publications/detail/actualites/identification-du-patient/
- 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. NOR : AFSH1318245J
- Référentiel national d'identitovigilance (RNIV)
- Référentiel INS

15 ANNEXES

Annexe A : EXIGENCES ET RECOMMANDATIONS ISSUES DU RNIV

Exi PP 01	L'appel au téléservice INSi est obligatoire pour vérifier une identité INS reçue lorsque l'identité numérique n'existe pas ou qu'elle ne dispose pas d'un statut récupéré ou qualifié.
Exi PP 02	La création d'une identité numérique requiert la saisie d'une information dans au moins 5 traits stricts : nom de naissance, premier prénom de naissance, date de naissance, sexe et lieu de naissance.
Exi PP 03	Les champs relatifs à la liste des prénoms de naissance et au matricule INS sont renseignés dès qu'il est possible d'accéder à ces informations : présentation d'un titre d'identité et/ou appel au téléservice INSi, dans les cas d'usage où l'emploi du matricule INS est requis et autorisé.
Exi PP 04	Il est nécessaire de renseigner le maximum de traits complémentaires, selon les consignes que chaque structure définit en fonction de ses besoins.
Exi PP 05	Avant toute intégration de l'identité INS dans l'identité numérique locale, il est nécessaire de valider la cohérence entre les traits INS renvoyés par le téléservice INSi et les traits de la personne physique prise en charge.
Exi PP 06	L'interrogation du téléservice INSi par l'intermédiaire de la carte vitale est le mode d'interrogation à privilégier chaque fois que possible.

Exi PP 07	L'attribution d'un niveau de confiance à toute identité numérique est obligatoire.
Exi PP 08	Afin d'utiliser une identité numérique de confiance, il est indispensable de s'assurer, a minima lors du premier contact physique de l'usager dans une
	structure, que les justificatifs d'identité présentés correspondent bien à la personne prise en charge.
Exi PP 09	Il est formellement interdit de procéder à la validation d'une identité numérique sans pouvoir contrôler sa cohérence à la lumière d'un titre d'identité à haut niveau de confiance, ou son équivalent numérique, dont le type est dument enregistré dans le système d'information.
Exi PP 10	Il doit être affiché a minima les traits stricts suivants : nom de naissance, premier prénom de naissance, date de naissance, sexe et, sur les documents comportant des données d'information de santé, le matricule INS suivi de sa nature (NIR ou NIA) lorsque cette information est disponible et que son partage est autorisé.
Exi PP 11	Dès lors que son identité est passée au statut Identité qualifiée, le matricule INS et les traits INS doivent être utilisés pour l'identification de l'usager, notamment lors des échanges de données de santé le concernant.
Exi PP 12	Les structures doivent disposer d'une cartographie applicative détaillant en particulier les flux relatifs aux identités. Les outils non interfacés nécessitant une intervention humaine pour mettre à jour les identités doivent être identifiés.
Exi PP 13	Une charte informatique formalisant les règles d'accès et d'usage du système d'information, et en particulier pour les applications gérant des données de santé à caractère personnel, doit être élaborée au sein de chaque structure à exercice collectif.
Exi PP 14	Les acteurs de santé impactés par la diffusion d'une erreur en lien avec l'identité INS doivent être alertés sans délai, selon une procédure spécifique formalisée par la structure.
Exi PP 15	Les structures de santé d'exercice collectif doivent formaliser la politique institutionnelle d'identification de l'usager au sein d'une charte d'identitovigilance.
Exi PP 16	Comme pour les autres traits stricts, la date de naissance à enregistrer est celle établie d'après un document ou un dispositif officiel d'identité et non celle lue sur un document de l'Assurance maladie, qui peut être différente.
Exi PP 17	L'enregistrement du nom utilisé est obligatoire lorsqu'il est différent du nom de naissance.

Exi PP 18	L'enregistrement du prénom utilisé est obligatoire lorsqu'il est différent du premier prénom de naissance.
Reco PP 01	Pour obtenir des résultats pertinents, il est fortement recommandé de limiter le nombre de caractères saisis pour effectuer la recherche d'un enregistrement.
Reco PP 02	Il est important que toute difficulté rencontrée pour la récupération de l'identité INS ou la qualification de l'identité numérique, du fait d'une incohérence non mineure, soient signalée comme événement indésirable et rapportée au niveau régional et national[1].

Les exigences posées par le RNIV viennent en compléments de celle posées par le référentiel INS.

Annexe B : REGIME JURIDIQUE APPLICABLE AU REFERENCEMENT DES DONNEES AVEC L'INS

Différentes obligations qui découlent directement du RGPD et la Loi relative à l'informatique aux fichiers et aux libertés (LIL) de 1978 sont formulées dans le référentiel.
Ainsi, on peut noter que les acteurs du cercle de confiance sont tenus de :

Respecter l'obligation de référencer les données avec l'INS

L'ensemble des acteurs faisant partie du cercle de confiance sont tenus de référencer les données de santé et les données administratives des personnes prises en charge à des fins sanitaires ou médico-sociales. L'INS ne peut être utilisé à d'autres fins que le référencement de ces données pour ces finalités.
Fondement légal de l'obligation : L'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales est obligatoire en application des articles L1111-8-1 et R1111-8-2 du CSP.
Dérogation légale de l'obligation : Le législateur a prévu un cas de dérogation à l'obligation d'utiliser l'INS en raison d'un obstacle légitime de procéder au référencement. Il s'agit du cas dans lequel il est impossible de procéder au référencement, par exemple dans le cas d'une prise en charge en urgence.
En outre, la dérogation à l'obligation légale d'utiliser l'INS peut provenir d'un texte s'opposant à l'identification (exemple : texte imposant l'anonymat).

[1] Les modalités de signalement aux niveaux régional et national seront précisées ultérieurement

Imbrication du traitement de référencement dans un traitement de données de santé :
L'opération de référencement des données de santé avec l'INS s'inscrit dans un la majorité des configurations dans un traitement de données de santé plus large ayant une finalité s'inscrivant nécessaire dans le domaine de la prise en charge sanitaire ou médico-sociale (mise en oeuvre dossier patient informatisé, traitement imagerie médicale, télésurveillance…).
De ce fait, l'article R1111-8-4 dispose que l'utilisation doit rester conforme à la finalité du référencement, exclusivement sanitaire ou médico-sociale (prise en charge médicale, suivi social, gestion administrative des personnes prises en charge).

Respecter la liste des données concernées par l'opération de référencement

• **L'INS :** L'obligation de référencement par l'INS n'impose pas une substitution aux autres identifiants locaux. Il n'est pas non plus exigé un remplacement des éléments d'identité déjà recueillis.

Les données présentes dans les bases de référence pourront donc s'y ajouter, en rappelant que la législation sur les données personnelles impose un principe de minimisation de ces données.

• **Les traits d'identité :** le nom de famille, le prénom, le sexe, la date de naissance et le lieu de naissance.

Transmettre les données référencées avec l'INS uniquement aux acteurs légitimes à en être destinataires

Une fois les données de santé référencées avec l'INS, elles ne peuvent être échangées et partagées que par les acteurs du Cercle de confiance et dans le respect des conditions de l'échange et du partage des données de santé (L1110-4 CSP).
Respecter les droits des personnes dont les données sont référencées avec l'INS

• Absence de droit d'opposition :
Les personnes dont les données sont référencées avec l'INS peuvent exercer les droits qu'elles détiennent en application du régime juridique applicable au traitement de données à caractère personnel (RGPD et LIL 1978).
Il est réglementairement prévu (R1111-8-5) que la personne concernée ne dispose pas de droit d'opposition au référencement de ses données de santé avec l'INS, afin de ne pas risquer de paralyser l'obligation d'utiliser l'INS. Pour autant, le droit d'opposition existe toujours, pour motif légitime, au profit de la personne concernée à l'égard par exemple de son dossier patient informatisé.

• Droit à l'information :
L'usager concerné par le référencement de ses données de santé par l'INS doit être informé de l'utilisation de l'INS par le responsable de l'obligation de référencement, qui doit tenir compte de son contexte d'usage.

Aussi l'information doit porter sur la présentation des objectifs poursuivis par l'utilisation de l'INS et sur l'absence de droit d'opposition.
Cette information doit être un élément d'une information plus large, délivrée au titre des modalités de prise en charge sanitaire ou du suivi médico-social dont la personne fait l'objet et des outils mis en oeuvre pour tracer cette prise en charge ou ce suivi (Articles 13 et 14 RGPD).

Respecter la durée de conservation

Pour déterminer la durée de conservation de l'INS, le responsable de l'obligation de référencement doit tenir compte de son contexte d'usage et des outils mis en oeuvre pour tracer cette prise en charge ou ce suivi.
En d'autres termes, l'INS permet le référencement de nombreuses données, et doit être conservé **aussi longtemps que les données qu'il référence** (INS, éléments d'identité, données de santé et données administratives).
Exemple de l'article R1112-7 : Le dossier médical mentionné à R1112-2 est conservé pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein