GRIVES
GROUPE INTERRÉGIONAL D'IDENTITOVIGILANCE EN SANTÉ
PACA - CORSE

CHARTE
D'IDENTITOVIGILANCE AZUREZO

AZUREZO

Ce document constitue la charte d'identitovigilance de l'outil régional de e-santé AZUREZO, de la région PACA. Il contient les règles de gestion de l'identité des usagers dans Azurezo qui doivent être appliquées par tous les professionnels utilisateurs de cet outil.

ars Agence Régionale de Santé Provence-Alpes Côte d'Azur

GRIVES GROUPE INTERRÉGIONAL D'IDENTITOVIGILANCE EN SANTÉ PACA - CORSE	CHARTE D'IDENTITOVIGILANCE AZUREZO	Type : Charte Version n° : 2 Date d'application : Page : 1 / 18
Rédaction : Dr Manuela OLIVER Fonction : Référent régional en identitovigilance Date : Septembre 2022	Validation : DAC PACA Fonction : Date : 21/11/2022	Approbation : PACA Fonction : Comité de pilotage de l'identitovigilance Date :
Diffusion le :	Destinataires : ARS, DAC, tous professionnels utilisateurs d'AZUREZO	

Indice de version	Date d'application	Objet de la révision
01	Septembre 2022	Création du document
02	Février 2023	Mise à jour de la charte graphique du document

SOMMAIRE

1 Introduction

L'identitovigilance est définie comme l'organisation et les moyens mis en œuvre par un établissement ou un professionnel de santé pour fiabiliser et sécuriser l'identification de l'usager à toutes les étapes de sa prise en charge.
Elle concerne :

- l'élaboration de documents de bonnes pratiques relatifs à l'identification de l'usager ;
- la formation et la sensibilisation des acteurs sur l'importance de la bonne identification des usagers à toutes les étapes de leur prise en charge ;
- l'évaluation des risques et l'analyse des événements indésirables liés à des erreurs d'identification ;
- l'évaluation des pratiques et de la compréhension des enjeux par l'ensemble des acteurs concernés (professionnels, usagers, correspondants externes).

Elle s'applique à toutes les étapes de prise en charge de l'usager en termes :

- d'identification primaire qui vise à attribuer une identité numérique unique à chaque usager dans le système d'information afin que les données de santé enregistrées soient accessibles chaque fois que nécessaire ;
- d'identification secondaire qui permet de garantir que le bon soin est administré au bon patient.

Cette charte d'identitovigilance a pour périmètre l'utilisation de l'outil Azurezo et ne concerne donc que l'identification primaire de l'usager.

La charte d'identitovigilance a pour objet de formaliser la politique conduite par les Dispositifs d'Appui à la Coordination (DAC) pour bien identifier les usagers pris en charge afin de garantir leur sécurité tout au long de leur parcours.
Elle définit l'organisation et les moyens mis en œuvre ainsi que les règles à respecter par l'ensemble des professionnels des DAC.

2 Politique d'identitovigilance

La maîtrise de l'identification des usagers est un enjeu majeur pour garantir la qualité et la sécurité de la prise en charge des usagers. 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 usagers.
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.

La région PACA accorde une importance particulière à la fiabilisation de l'identification de l'usager et définit l'identification comme un acte de soin à part entière.

2.1 Mode de prise en charge

La politique d'identification de l'usager dans Azurezo s'applique aux prises en charge et parcours utilisant cet outil.

2.2 Acteurs concernés

L'usager est directement concerné par son identification et doit être acteur de ses soins et de sa prise en charge.
Les professionnels concernés sont ceux qui prennent en charge directement l'usager et ceux qui interviennent sur tout ou partie des données médico-administratives de l'usager (identification primaire) :

- professionnels des Dispositifs d'Appui à la Coordination (DAC) ;
- professionnels libéraux ou hospitaliers utilisant cet outil (médecins, infirmiers, kinésithérapeutes, sage-femmes, assistantes médico-administratives…) ;
- professionnels de la Cellule Régionale d'Identitovigilance (CRIV).

2.3 Système d'information

La politique d'identitovigilance concerne l'outil Azurezo qui est mis en œuvre par le Groupement Régional d'Appui au Développement de la e-Santé (GRADeS) innovation e-santé Sud (ieSS).

3 Gouvernance de l'identitovigilance

La gouvernance régionale de l'identitovigilance est décrite dans le document « politique et gouvernance régionale de l'identitovigilance en région PACA ».
Aux instances décrites dans le document cité supra, s'ajoutent :

- le comité consultatif des utilisateurs Azurezo ;
- le chef de programme Azurezo.

3.1 Comité consultatif des utilisateurs Azurezo

Ils représentent les utilisateurs de la solution Azurezo.
Le comité consultatif comprend *a minima* :

- un représentant de chaque Dispositif d'Appui à la Coordination (DAC) ;
- le référent régional en identitovigilance ;
- le chef de programme Azurezo ;

Ce comité consultatif est aussi ouvert à d'autres acteurs que les DAC. Il peut s'agir de professionnels de santé hôpital, ville, coordinateurs CPTS…
Ce comité se réunit deux fois par an.
Il étudie les problématiques rencontrées concernant l'identification de l'usager (évènements indésirables relatifs à l'identification primaire), remontées par la cellule régionale d'identitovigilance.
Il étudie les indicateurs de qualité du référentiel identité et peut proposer des actions d'amélioration qui seront arbitrées par le comité stratégique régional en identitovigilance.

3.2 Référent logiciel

Un référent logiciel est désigné, il s'agit du chef de programme Azurezo exerçant au sein de ieSS. Le référent logiciel :

- participe en lien avec la CRIV aux tests d'interfaces d'identités ;
- informe la CRIV de toute montée en version d'Azurezo susceptible d'impacter la gestion de l'identité et collabore avec la CRIV à la mise en œuvre des tests destinés à vérifier le bon fonctionnement ;
- informe la CRIV de toute anomalie liée à l'identité dont il serait informé :
    - par l'éditeur,
    - par les utilisateurs.
- Collabore avec le correspondant en identitovigilance désigné au sein des DAC

3.3 Correspondant en identitovigilance au sein des DAC

Un correspondant en identitovigilance est identifié au sein de chaque DAC.

- Formé par la CRIV, il est son correspondant privilégié au sein des DAC pour tous les sujets liés à l'identification des usagers dans Azurezo ;
- Il contribue à la formation continue des personnels des DAC en collaboration avec la CRIV ;
- Il s'assure de l'application des bonnes pratiques d'identification primaire par les professionnels des DAC ;
- Il assure le support de premier niveau pour les personnels des DAC pour toutes les questions concernant l'identification primaire ;
- Il sollicite si nécessaire la CRIV pour un avis d'expert sur des cas complexes ;
- Il promeut le signalement des évènements indésirables et participe à leur analyse ;
- Il participe avec la CRIV, aux retours d'expériences organisés.

4 Définitions et terminologies

L'objet de ce chapitre est de rappeler la signification des termes techniques utilisés dans le domaine de l'identification de l'usager. Les termes employés en identitovigilance sont définis dans l'annexe II du volet socle du RNIV *(Principes d'identification des usagers communs à tous les acteurs de santé*). Il n'en sera précisé que certains dans cette charte qui ont une importance toute particulière en termes de qualité et de sécurité de la prise en charge.

4.1 Identification

Identifier une personne consiste à disposer des informations nécessaires et suffisantes pour ne pas confondre cette personne avec une autre. Cela consiste à recueillir les informations (traits) représentant une personne physique pour l'identifier de façon unique. Ces traits d'identification sont utilisés comme critères pour rechercher l'usager dans le système d'information. Ils concourent à la sécurité de sa prise en charge.

4.2 Identité et identifiant numériques

Identité numérique : L'identité numérique correspond à la représentation d'un individu physique dans un système d'information. Un même usager physique est ainsi associé à plusieurs identités numériques selon le système d'information utilisé : employeur, impôts, sécurité sociale, mutuelle, banque, etc.

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.

Identité nationale de santé (INS) : L'identité nationale de santé (INS) est une identité numérique qui repose sur des bases nationales de référence. Chaque identité INS comprend les éléments suivants :

- le matricule INS qui a pour valeur le NIR (ou le NIA) personnel de l'usager, sur 15 caractères ;
- les traits INS qui sont les traits d'identité de référence associés au NIR/NIA dans les bases de référence (nom de naissance, prénom(s), sexe, date de naissance et code INSEE du lieu de naissance) ;
- l'organisme qui a affecté l'INS, précisé sous la forme d'un OID (object identifier), information habituellement invisible pour le professionnel de santé (le NIR et le NIA ayant chacun leur autorité d'affectation, cela permet de les distinguer).

4.3 Domaine d'identification

Le domaine d'identification (DI) d'Azurezo est un domaine d'identification unique.

4.4 Traits d'identification

Les traits d'identification sont les éléments constituant l'identité d'un usager. On distingue :

- les traits stricts : ce sont les informations de référence qui caractérisent l'identité officielle de l'usager ; elles permettent de référencer les données de santé partagées et de fiabiliser les rapprochements d'identités numériques entre structures. Les traits stricts sont stables dans le temps.
- les traits complémentaires : ce sont des données qui apportent d'autres informations utiles à la prise en charge de l'usager mais qui sont plus variables dans le temps.

4.5 Statuts des identités

Les statuts de l'identité sont utilisés pour attribuer un niveau de confiance à l'identité numérique. On distingue 4 statuts :

- Identité provisoire : statut de plus bas niveau de confiance d'une identité, il correspond à une identité créée localement sans contrôle de cohérence avec un dispositif d'identification de haut niveau de confiance. Il s'agit du statut attribué par défaut à toute identité nouvellement créée localement.
- Identité validée : ce statut correspond à une identité créée localement dont la cohérence a été contrôlée à l'aide d'un dispositif d'identification de haut niveau de confiance. L'attribution du statut identité validée est une action manuelle et volontaire du professionnel

- Identité récupérée : Ce statut caractérise une identité créée ou modifiée par appel au téléservice INSi et récupération de l'INS, les traits de l'identité sont ceux de l'INS. Toutefois le contrôle de cohérence de ces traits avec ceux présents sur un dispositif d'identification de haut niveau de confiance n'a pas été réalisé.
- Identité qualifiée : statut de plus haut niveau de confiance, d'une identité et seul statut permettant l'utilisation du matricule INS (et de l'OID) pour référencer, échanger et partager des données de santé, il correspond à une identité créée ou modifiée par appel au téléservice INSi et récupération de l'INS et dont la cohérence a été contrôlée à l'aide d'un dispositif d'identification de haut niveau de confiance.

4.6 Doublons, fusions, collisions

Un doublon d'identités numériques correspond à l'identification d'une même personne physique sous au moins deux identifiants différents dans un même domaine d'identification (DI).
Les informations d'un même usager sont donc réparties dans plusieurs dossiers différents qui ne communiquent pas entre eux. L'équipe soignante ne dispose donc pas de l'ensemble des informations qui peuvent être nécessaires à la prise en charge.
Lors du dépistage d'un doublon, celui-ci est tout d'abord qualifié de doublon potentiel. L'étude des deux dossiers permet de déterminer s'il s'agit réellement d'un doublon (doublon avéré) ou d'homonymes dans le cas contraire.

La fusion correspond au traitement des doublons avérés. Elle consiste à regrouper toutes les informations d'un même individu sous un identifiant numérique unique. L'Identifiant Permanent Patient (IPP) conservé est alors appelé IPP maître et l'IPP fusionné devient l'IPP esclave ou fantôme selon les systèmes d'informations.

La collision correspond à la présence, sous un même identifiant numérique, d'informations issues de deux usagers différents. On distingue la collision primaire qui peut résulter d'une erreur de choix de dossier patient lors d'une venue, être la conséquence de l'utilisation frauduleuse d'une identité par un autre individu ou être la conséquence d'une fusion réalisée avec des critères insuffisants (collision secondaire).

5 La gestion de l'identité

5.1 Domaine d'identification

La région PACA dispose d'un référentiel unique d'identité, le serveur régional d'identité et de rapprochement (SRIR). Les identités peuvent être transmises à Azurezo si l'identité de l'usager pris en charge est connue dans le SRIR et sélectionnée par le professionnel. Toutes les identités créées dans AZUREZO alimentent le SRIR.
La cartographie applicative des outils régionaux de la région PACA décrit les interfaces existantes entre les applicatifs utilisés. Toutes les interfaces sont des interfaces normées, respectant le cadre d'interopérabilité des systèmes d'information en santé et le standard IHE PAM.

5.2 Identifiants utilisés en région

Les identifiants numériques utilisés en région sont :
- l'identifiant permanent patient régional (IPPR), identifiant unique de l'usager, associé à son identité ; (93 + 10 chiffres) ;
- l'identifiant interne d'Azurezo (incrémental à partir de 1).

5.3 Création des identités

Les identités peuvent être créées par tout professionnel de santé participant à la prise en charge :
- professionnels des dispositifs d'appui à la coordination (DAC) ;
- les professionnels alimentant le dossier communicant de cancérologie (professionnels de la cancérologie et notamment ceux des centres de coordination en cancérologie (3C)) ;
- tous les professionnels utilisant l'outil Azurezo ;
- professionnels libéraux (médecins, kinésithérapeutes, sage-femmes, infirmiers…) ;
- professionnels des établissements de santé (médecins ou assistants médico-administratifs).

Les lieux de création d'identités sont divers :

- cabinet médical ;
- établissement de santé ;
- dispositif d'appui à la coordination ;
- domicile de l'usager ;
- établissement médico-social (EHPAD, MDPH…)

5.4 Les traits d'identification

La région PACA respecte les exigences du RNIV en matière de traits d'identification utilisés dans l'outil Azurezo. Les traits d'identification utilisés sont les suivants :

5.4.1 Traits stricts

- Nom de naissance ;
- Premier prénom de naissance ;
- Date de naissance ;
- Sexe ;
- Le code INSEE du lieu de naissance : le système d'information propose automatiquement un code de lieu de naissance si la ville et/ou le code postal ou le pays de naissance sont saisis ;
- Matricule INS (toujours associé à son OID[1]).

5.4.2 Traits complémentaires

- *Nom utilisé* (saisie obligatoire si différent du nom de naissance) que si présent sur la PI ;
- Liste des prénoms de naissance figurant sur la PI ;
- *Prénom utilisé* (saisie obligatoire si différent du premier prénom de naissance) ;
- Type de document d'identité présenté ;
- Adresse courriel (e-mail) ;
- Numéro de téléphone mobile.
- Adresse de l'usager ;
- Ajout de numéros de téléphone supplémentaires (mobile, domicile, bureau, fax) ;
- Numéro de sécurité sociale.

5.4.3 Politique concernant la saisie des noms et prénoms utilisés

La région PACA a fait le choix de saisir à l'identique les éléments d'identité présents sur la pièce d'identité présentée par l'usager. Cela signifie qu'il est nécessaire de :

- saisir un nom utilisé s'il est mentionné sur la pièce d'identité, y compris si l'usager ne le souhaite pas. L'usager sera alors informé qu'il lui appartient de faire modifier sa pièce d'identité ;
- saisir un prénom utilisé uniquement si celui-ci est mentionné sur la pièce d'identité :
    - Ce prénom fait partie des prénoms de naissance (article 57 du code civil, tout prénom de naissance peut être utilisé comme prénom usuel),
    - ce prénom, bien qu'il ne fasse pas partie des prénoms de naissance est explicitement mentionné sur la pièce d'identité (prénom usuel : XXX).

5.4.4 Politique concernant le double nommage

Le double nommage (c'est-à-dire la recopie systématique d'un nom de naissance dans le champ nom utilisé si l'usager utilise son nom de naissance dans la vie courante) n'est pas pratiqué. Pour un usager utilisant uniquement son nom de naissance, le champ *nom utilisé* ne sera pas renseigné.

[1] *Object identifier* : identifiant numérique spécifique associé au matricule INS qui permet de distinguer sa nature : NIR ou NIA

5.5 Recherche, création, qualification d'une identité

5.5.1 Principes généraux

Les professionnels utilisateurs recherchent l'identité de l'usager dans Azurezo puis dans le SRIR si l'identité de cet usager n'est pas connue dans Azurezo
Les créations d'identité se font dans Azurezo puis sont transmises au référentiel régional d'identité (SRIR).

5.5.2 Accueil de l'usager

Tout professionnel de l'accueil demande à l'usager de décliner son identité par question ouverte y compris si l'usager présente une pièce d'identité.

5.5.3 Recherche d'une identité

Conformément au RNIV, la recherche d'une identité est réalisée par la saisie de la date de naissance.

Compte tenu de la taille du référentiel identité et afin de diminuer les temps de recherche, le professionnel peut compléter la date de naissance par les 3 premiers caractères du nom et par les 3 premiers caractères du prénom.
Si l'usager fait partie de sa file active, l'identité s'affichera.
Néanmoins, pour les usagers n'appartenant pas à la file active du professionnel, ce dernier devra saisir intégralement les traits suivants :

- nom de naissance,
- premier prénom de naissance ;
- date de naissance ;
- sexe.

Cela permet également de respecter les obligations de confidentialité et de secret médical.
Aussi, si une première recherche respectant les bonnes pratiques (date de naissance, début du nom, début du prénom) est infructueuse, le professionnel est invité à renseigner complètement les traits stricts mentionnés ci-dessus avant de réitérer la recherche.
Si aucune identité n'est proposée, la recherche est alors étendue à l'ensemble des identités présentes dans le référentiel régional d'identité.

Le système d'information permet la recherche d'une chaîne de caractères à la fois dans les champs nom de naissance et nom utilisé pour le nom et dans les champs prénoms de naissance et prénom utilisé pour le prénom.

5.5.4 Création d'une identité

Une identité locale est systématiquement créée. L'appel au téléservice INSi est réalisé en back-office par les personnels de la CRIV.

Conformément au RNIV, les traits obligatoires pour créer une identité sont :

- le nom de naissance ;
- le premier prénom de naissance ;
- le sexe ;
- la date de naissance ;
- le code INSEE du lieu de naissance : le système d'information propose automatiquement un code de lieu de naissance si la ville et/ou le code postal ou le pays de naissance sont saisis.

Si le lieu de naissance est inconnu, le professionnel saisit le code 99999 dans le champ "commune de naissance".

Ces traits stricts sont obligatoirement complétés par :

- la liste des prénoms de naissance ;
- le matricule INS et son OID ;

dès que l'appel au téléservice a pu être réalisé pour les usagers éligibles[2].

[2] Usagers nés ou travaillant en France

Les traits stricts sont aussi complétés par les traits complémentaires suivants :

- adresse de l'usager ;
- adresse courriel (e-mail) ;
- numéro(s) de téléphone ;

Le processus détaillé de création d'une identité est décrit dans la fiche réflexe Azurezo "Recherche et création d'une identité". Seuls les éléments structurants sont repris ici.

5.5.4.1 Les règles de saisies de l'identité

Les champs nom de naissance, nom utilisé, premier prénom, liste des prénoms, prénom utilisé sont saisis en majuscule sans caractères accentués ou diacritiques. Tirets et apostrophes sont conservés.

5.5.4.2 L'utilisation de l'opération de récupération du téléservice INSi.

L'appel au téléservice INSi est réalisé dans le SRIR par la CRIV. Ces opérations sont encadrées par un contrat de sous-traitance entre les DAC et le GRADeS ieSS porteur de la CRIV.
La région a fait le choix d'appeler le téléservice INSi pour les identités au statut d'identité provisoire et a mis en place une organisation de validation des identités en back office.

L'appel au téléservice par saisie des traits est privilégié (les personnels de la CRIV, en charge de la récupération de l'INS, n'ayant pas accès à la carte vitale de l'usager).

5.5.5 Attributs de l'identité

Les attributs décrits ci-dessous peuvent être utilisés dans le référentiel identité.

- *identité douteuse* : cet attribut est utilisé lors d'une suspicion d'utilisation frauduleuse d'identité par un usager (usurpation d'identité) ;
- *identité fictive* : cet attribut permet de caractériser une identité numérique ne reposant pas sur les traits réels de l'usager pris en charge (usagers souhaitant être pris en charge de façon anonyme en particulier). Le processus détaillé de création d'une identité fictive est décrit dans la fiche réflexe Azurezo "Création d'une identité fictive" ;
- *identité homonyme* pour attirer l'attention des professionnels sur la présence d'identités approchantes dans le référentiel identité.

Ces attributs doivent être saisis dans Azurezo et sont transmis au SRIR. Ils peuvent également être saisis directement dans le SRIR par les personnels de la CRIV si nécessaire.

Pour mémoire : les attributs *identité douteuse* ou *identité fictive* interdisent la validation de l'identité et l'appel au téléservice INSi.

5.5.6 Processus de validation des identités et de qualification de l'INS

Si l'usager est physiquement présent lors de la création de l'identité, ou si le professionnel se déplace au domicile de l'usager, la validation est réalisée au vu d'une pièce d'identité de haut niveau de confiance par le personnel qui crée ou modifie l'identité. L'usager doit avoir présenté un dispositif d'identification à haut niveau de confiance.

Si le patient n'est pas physiquement présent, ou si le professionnel n'a pas procédé à la validation de l'identité, cette validation est réalisée en back office par la CRIV après réalisation d'un contrôle de cohérence entre l'identité numérique et l'identité présente sur la pièce d'identité si celle-ci est disponible dans le référentiel identité.
Si aucune pièce d'identité n'est disponible, l'usager est sollicité par mail ou SMS pour réaliser une identification électronique de niveau substantiel au sens du règlement européen eIADS[3].

Ces opérations de gestion des identités sont organisées *via* un contrat de sous-traitance.

[3] Electronic IDentification Authentification and trust Services

5.5.7 Les dispositifs d'identification à haut niveau de confiance

Les dispositifs d'identification à haut niveau de confiance conformément au RNIV sont les suivants :

- carte nationale d'identité pour les usagers français et les ressortissants de l'Union Européenne ;
- carte nationale d'identité des ressortissants des pays "voisins" qui ne font pas partie de l'UE (Principauté Monaco, Principauté d'Andorre, Principauté de San Marin, Etat du Vatican, Suisse, Norvège, Islande et Liechtenstein) ;
- passeport ;
- titre de séjour ;
- pour les mineurs, livret de famille ou extrait d'acte de naissance accompagné de la pièce d'identité du responsable légal ;
- pour une personne âgée en EHPAD, acte de naissance et la PI d'un parent (descendant en règle générale) ;
- dispositif d'identification électronique de niveau substantiel (au sens du règlement européen eIADS).

Les pièces d'identités peuvent être numérisées dans Azurezo. Ces pièces sont conservées dans le référentiel régional d'identité et dans Azurezo dans les conditions précisées dans la FP06 Gestion des copies de pièces d'identité dans le système d'information proposée par le réseau 3RIV.

5.5.8 Identités particulières

5.5.8.1 Cas de l'anonymat

Les usagers doivent être créés nominativement dans l'application AZUREZO pour bénéficier de la prise en charge. Néanmoins, dans certains cas, l'identité de l'usager est inconnue ou celui-ci souhaite être pris en charge de façon anonyme.
Dans ce cas, il convient donc d'avoir recours aux identités fictives.
Dans la mesure du possible, il est recommandé de limiter au maximum les cas de recours aux identités fictives. Toutes les DAC partageant maintenant le même outil et par conséquent le même référentiel identité, il est indispensable de prévoir le recours aux identités fictives afin :

- d'éviter l'utilisation d'une même identité fictive par plusieurs DAC et donc la collision de données médicales ou paramédicales appartenant à des usagers différents dans le même dossier informatique ;
- que ces identités fictives soient facilement repérables dans le SRIR par la CRIV.

Les règles de nommages à respecter sont les suivantes :
Nom de naissance : Abréviation du DAC- La première lettre du prénom et les 2 premières lettres du nom de l'opérateur-date du jour (jj-mm-aaaa)-numéro chrono (à réinitialiser chaque jour).
Prénom : Anonyme
Date de naissance : 01/01/AAAA (année réelle) de préférence ou 01/01/AAAA (décennie estimée)
Sexe : Sexe de l'usager ou I (si inconnu ou indéterminé)
Lieu de naissance : 99999

5.5.8.2 Cas des identités tests

Les tests informatiques sont réalisés en préproduction. Toutefois, dans le cadre de la formation des personnels, il peut être nécessaire d'utiliser en base de production des identités tests.
La CIV doit être informée par le correspondant en identitovigilance des DAC de la création d'une identité test.
Les règles de nommage suivantes doivent être respectées :
Nom de naissance : Nom du DAC suivi de la date du jour au format AAAAMMJJ
Nom utilisé : TEST
Prénom : à discrétion de l'utilisateur
Date de naissance : à discrétion de l'utilisateur
Lieu de naissance : à discrétion de l'utilisateur

5.6 Identification primaire sans présence physique de l'usager.

Les professionnels des DAC créent le plus souvent l'identité d'un usager à la suite d'une sollicitation téléphonique (d'un professionnel, de l'usager, de sa famille). La validation de l'identité et la qualification de l'INS ne peuvent se faire que dans un second temps :

- soit lors de la rencontre de l'usager et du professionnel (cas des MAIA par exemple) ;
- soit après sollicitation de l'usager par la CRIV (identification électronique de niveau substantiel (cf.6.2.4).

Lors de la création de l'identité sur sollicitation téléphonique et afin de limiter les erreurs, il est demandé aux professionnels de poser des questions ouvertes et précises (quel est votre nom de naissance ? Quel est votre premier prénom ? …), de faire épeler puis de répéter la saisie. En présence d'un nom ou d'un prénom composé, il est nécessaire de faire préciser à l'usager la présence ou non d'un tiret.

5.7 Signalement et traitement des anomalies d'identité

Le maintien de la qualité du référentiel identité est sous la responsabilité de :

- chaque utilisateur qui doit signaler les anomalies qu'il dépiste ;
- de la CRIV qui, dans le cadre d'un contrat de sous-traitance avec les utilisateurs, doit traiter les anomalies signalées et mettre en œuvre les outils informatiques de dépistage des anomalies (algorithme de recherche de doublons…).

Tous les professionnels sont formés et incités à la déclaration des anomalies :

- erreur d'identité ;
- doublon potentiel ;
- collision potentielle ;
- erreur d'attribution d'une INS.

Le signalement des anomalies d'identités est réalisé directement dans Azurezo. La conduite à tenir est précisée dans la fiche réflexe "Signalement des anomalies d'identité".

5.8 Droits d'identification

Les droits d'identification des personnels sont décrits dans le tableau ci-dessous.

Professionnel	Utilisateurs Azurezo	Cellule régionale d'identitovigilance (CRIV)
Application utilisée	Azurezo	Référentiel régional d'identité
Recherche et consultation d'une identité	X	X
Création identité locale	X	X
Appel au téléservice INSi		X
Modification d'identité (non qualifiée)	X	X
Validation d'identité	X	X
Fusion Défusion de collision		X
Déqualification, suppression d'une INS		X

6 Identification secondaire

6.1 Intégration d'éléments dans le dossier de l'usager

Les professionnels peuvent devoir intégrer des éléments extérieurs dans le dossier de l'usager :

- pièce d'identité transmise ;
- ordonnance ;
- données d'examens médicaux (ECG par exemple dans le cadre d'une demande d'expertise en télémédecine, photographie d'une plaie…).

Tous ces éléments extérieurs doivent être identifiés avec les traits minimaux d'identités de l'usager exigés par le RNIV (nom de naissance, premier prénom de naissance, sexe, date de naissance) pour éviter les erreurs.

L'intégration de ces éléments doit respecter les bonnes pratiques d'identitovigilance :

- recherche du dossier par date de naissance complétée éventuellement des 3 premières lettres d'nom et/ou du prénom
- vérification de la cohérence de l'identité du dossier avec celle du document à intégrer.

6.2 Identification des documents du dossier de l'usager

Les documents produits dans Azurezo et pouvant être imprimés comportent sur toutes les pages l'identité complète de l'usager, à savoir :

- nom de naissance
- nom utilisé si celui-ci est différent du nom de naissance ;
- premier prénom de naissance ;
- liste des prénoms si l'usager dispose d'une INS qualifiée ;
- prénom utilisé si celui-ci est différent du premier prénom ;
- date de naissance ;
- sexe ;
- code géographique officiel et nom de ville ou de pays du lieu de naissance.
- matricule INS accompagné de sa nature (NIR ou NIA) si l'usager dispose d'une INS qualifiée.

7 La gestion documentaire

L'ensemble de la documentation (procédures, modes opératoires, enregistrements) relative à l'identitovigilance sont disponibles dans l'outil de gestion documentaire du GRADeS ieSS.
L'alimentation de la gestion documentaire est sous la responsabilité de la CRIV qui sollicite le chef de programme Azurezo pour la rédaction et la mise à jour des documents. Les fiches réflexes et documents socles sont disponibles pour les professionnels des DAC dans l'onglet documentation du site internet https://ies-sud.fr/azurezo/

7.1 Procédures

Il existe des procédures concernant l'identification des usagers dans Azurezo.

7.2 Fiches réflexes

Des fiches réflexes d'identitovigilance sont mises à disposition des DAC par la cellule régionale d'identitovigilance.

- Recherche et création d'une identité dans Azurezo
- Conduite à tenir devant une identité particulière
- Création d'une identité fictive
- Mémento identitovigilance

7.3 Enregistrements de la CRIV

La CRIV possède et diffuse les enregistrements qui sont disponibles dans la gestion documentaire tels que les :

- documents réglementaires et techniques (fiches du réseau 3RIV, fiches GRIVES…) ;
- comptes-rendus de réunion ou relevé d'information de décision et d'action (RIDA) des instances (COSTRATIV, CRIV, comités consultatifs des utilisateurs) ;
- supports de formations ;
- support de communication et de sensibilisation (affiches, flyers…) ;
- cartes d'identité des indicateurs ;
- plan d'actions ;
- bilan d'activité ;
- cartographie des risques a priori ;
- tableau de bord des indicateurs ;
- comptes-rendus des analyses réalisées suites à la survenue d'évènements indésirables (Retours, d'expérience, …).

8 Pilotage

La CRIV suit des indicateurs relatifs à l'identification primaire dans Azurezo. Chaque indicateur dispose d'une carte d'identité disponible dans la GED.
Les indicateurs sont rassemblés dans un tableau de bord et sont suivis trimestriellement à l'exception du taux de formation du personnel qui est suivi annuellement. Le tableau de bord des indicateurs est tenu à jour par la CRIV et présenté à chaque réunion du COSTRIV.
Selon les résultats, la CRIV peut proposer la mise en place d'actions d'amélioration en accord avec les comités consultatifs des utilisateurs. Ces actions sont présentées et validées en COSTRIV.

8.1 Indicateurs d'identification primaire

Les indicateurs suivis pour le référentiel régional d'identité sont les suivants :

- taux d'identités au statut identité qualifiée ;
- taux d'identités au statut identité récupérée ;
- taux d'identités au statut identité validée ;
- taux d'identités au statut identité provisoire ;
- taux de doublon de flux ;
- nombre et/ou taux de collision ;
- nombre et/ou taux d'usurpation d'identité ;
- rapport fusion sur doublon avérés ;
- nombre d'erreurs d'identités ;
- taux d'évènements indésirables graves ayant pour origine une erreur d'identification primaire des usagers
- taux d'évènements porteurs de risques ayant pour origine une erreur d'identification primaire des usagers.

8.2 Formation du personnel

Le taux de formation du personnel (formation GRIVES) est suivi par les DAC et communiqué à la CRIV.

8.3 Évaluation et amélioration des pratiques professionnelles

La CRIV, en accord avec les comités consultatifs des utilisateurs, propose annuellement aux DAC de réaliser un audit de pratique relatif à l'identification primaire.

La réalisation de l'audit est sous la responsabilité du correspondant en identitovigilance du DAC. L'exploitation et l'analyse sont réalisées par la CRIV. Les résultats sont communiqués lors des comités utilisateurs.
Des actions d'amélioration sont proposées si nécessaire et validées par le comité utilisateur et mises en œuvre par la CRIV et les correspondants en identitovigilance des DAC.
Les résultats sont restitués au personnel.

9 La gestion des risques

9.1 La gestion des risques *a priori*

9.1.1 La veille réglementaire et technique

La CRIV réalise une veille réglementaire et technique en utilisant les ressources disponibles (liste non exhaustive) :

- journal officiel et bulletins officiels ;
- consultation du site de l'Agence du Numérique en Santé (ANS) ;
- communication des éditeurs ;
- participation aux travaux nationaux relatifs à l'identitovigilance ;
- participation aux manifestations nationales ou d'autres régions relatives à l'identitovigilance.

9.1.2 Modalités d'attribution et de gestion des droits d'accès informatiques

Les droits d'accès et les habilitations sont renseignés dans la matrice des droits Azurezo.

9.1.3 Traçabilité des actions

L'ensemble des applications informatiques participant à la prise en charge de l'usager disposent de fonctionnalités d'enregistrement horodaté des accès précisant le nom (login), le type d'accès (lecture ou écriture), les documents consultés. L'ensemble des actions réalisées sur les identités sont tracées, historisées et conservées pendant la durée de vie du dossier.

9.1.4 Fiabilisation des interfaces d'identités

Le GRADeS ieSS met en œuvre des procédures de test des interfaces d'identités entre Azurezo et le SRIR. Ces tests sont conduits par la CRIV, l'équipe projet Azurezo en relation avec le ou les éditeurs avant la mise en production de la version. Les tests sont mis en œuvre à chaque changement de version majeure d'un outil ou de l'EAI régional.

Une procédure encadre la réalisation de ces jeux d'essais.

9.1.5 Détection des utilisations frauduleuses d'identités

La région porte une attention particulière au risque d'utilisation frauduleuse d'une identité. Les personnels sont formés et mettent en œuvre des contrôles permettant de suspecter une utilisation frauduleuse d'identité.
La conduite à tenir devant une suspicion est formalisée et connue des personnels.
La conduite à tenir lors d'une suspicion de fraude comprend des mesures de sécurisation telles que :

- la création d'un dossier provisoire pour ne pas risquer de collision avec un dossier précédent ;
- le signalement interne de l'événement indésirable ;
- l'identification des documents présents dans le dossier et qui n'appartiennent pas à l'usager ;
- l'information des structures et professionnels avec lesquels les données ont été partagées ;
- l'isolement du ou des documents dans un dossier créé spécifiquement et tagué "identité douteuse" dans l'outil régional concerné.

9.2 Gestion des risques *a posteriori*

Les évènements indésirables en identification primaire en lien avec l'utilisation d'Azurezo doivent être signalés.
Un formulaire de signalement associé au dossier permet de réaliser le signalement à la CRIV et de conserver une trace dans le dossier concerné.

Les évènements indésirables graves font systématiquement l'objet d'une analyse utilisant une méthode ALARM. La CRIV est accompagnée par la structure d'appui à la qualité (PASQUAL PACA Corse) pour la réalisation des analyses. Les événements porteurs de risques récurrents sont également analysés.

Le référent en identitovigilance et la CRIV sont destinataires des fiches de signalement. Ils sont responsables de leur qualification (gravité) et de leur analyse. Ils proposent si nécessaire la mise en place d'un plan d'actions d'amélioration et participent à la mise en œuvre des actions.

Les événements indésirables graves sont signalés sur le portail national de signalement des événements sanitaires indésirables.
L'analyse des évènements indésirables permet de réactualiser annuellement la charte d'identitovigilance régionale. DE

9.3 Formation des professionnels

Lors de la formation des professionnels à l'utilisation d'Azurezo, une formation pratique d'utilisation est dispensée par les équipes projets concernées. Des fiches réflexes sont fournies aux professionnels, rappelant les bonnes pratiques d'identification primaire.
Tous les professionnels utilisateurs d'Azurezo sont invités à suivre une formation spécifique en identitovigilance, plus particulièrement en identification primaire.
La formation est dispensée par la CRIV sous forme de webinaires. Elle comprend les éléments suivants :

- présentation de la gestion documentaires (principales procédures et organisation de la gestion documentaire) ;
- formation aux bonnes pratiques d'identitovigilance primaire ;
- gestion des risques a priori avec en particulier une présentation des principaux risques en identification primaire ;
- gestion des risques a posteriori avec en particulier la déclaration des évènements indésirables (quels évènements déclarer, comment déclarer un évènement indésirable, intérêt de déclarer et d'analyser les événements indésirables).

Le programme des formations proposé est défini semestriellement par la CRIV et communiqué aux professionnels (le catalogue de formation du GRIVES est disponible dans l'espace agora social club et sur le site internet).

A l'issue de la formation, les professionnels sont invités à répondre à un quiz d'évaluation des connaissances acquises. Les professionnels obtenant plus de 50% de bonnes réponses se voient remettre une attestation de formation.
Une attestation de participation est également remise à tous.

Les professionnels sont invités à suivre une formation de remise à niveau tous les trois ans.

9.4 Actions de sensibilisation et de communication auprès des professionnels

Des actions de sensibilisation sont menées en région :

- les journées du GRIVES régionales et thématiques ;
- proposition d'affiches et de flyers de sensibilisation ;
- communication au cours de la journée annuelle du GRIVES et des comités d'utilisateurs portant sur les bonnes pratiques, les erreurs fréquemment rencontrées, les presque accidents ou événements porteurs de risques, analyse des événements indésirables ;
- newsletters.

10 Respect des droits de l'usager, information et sensibilisation

10.1 Respect des droits de l'usager

Le GRADeS ieSS se conforme à la réglementation relative aux droits des usagers du système de santé ainsi qu'à la réglementation relative à la protection des données à caractère personnel et notamment le règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ou RGPD).
Le consentement de l'usager est recueilli avant toute création de son dossier. La case "J'atteste que le patient est consentant à la création de ce dossier" doit être cochée.

Une information sur l'utilisation du dispositif régional d'identitovigilance est mise à disposition de l'usager. Cette information explicite notamment les principes de partage des données d'identification personnelles dans le cadre régional et les organisations mises en œuvre pour respecter les droits de l'usager et tout particulièrement :

- le droit d'être informé en cas de traitement des informations le concernant et notamment de l'utilisation de l'INS par les professionnels de santé pour échanger et partager des données et de l'impossibilité de s'opposer à l'utilisation de l'INS (obligation légale) ;
- le droit d'avoir accès aux informations médicales le concernant ;
- le droit de demander la rectification des données erronées ou périmées ;
- le droit d'avoir la garantie de la confidentialité des informations le concernant.

10.2 Maîtrise de l'identité – engagement des professionnels

Les professionnels s'engagent à respecter les bonnes pratiques d'identitovigilance et désignent le GRADeS ieSS comme sous-traitant pour la gestion des identités.

10.3 Information et sensibilisation des usagers

Une attention toute particulière doit être portée à la communication réalisée auprès des usagers et de leur famille afin de leur permettre de connaître leurs droits et de comprendre l'importance de l'identitovigilance.

11 Actualisation de la charte et de la politique d'identitovigilance

Cette charte est révisée annuellement pour prendre en compte :

- les évolutions réglementaires ;
- l'évolution des pratiques professionnelles ;
- l'évolution du contexte local ;
- l'évolution d'Azurezo ;
- les résultats des évaluations et des indicateurs ;
- les évènements indésirables, leur analyse et les plans d'actions mis en place.

12 Références bibliographiques

Seules sont reprises ici les références bibliographiques majeures,
L'ensemble des références présentes dans le volet 1 du RNIV doivent être consultées et à disposition de la structure.

- Arrêté du 27 mai 2021 (Journal officiel du 8 juin 2021) portant approbation des modifications apportées au référentiel « identifiant national de santé »
- Référentiel national d'identitovigilance (RNIV)
- Guide d'implémentation de l'INS à l'usage des éditeurs
- Arrêté du 24 décembre 2019 portant approbation du référentiel « Identifiant national de santé »
- Décret 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) comme identifiant national de santé
- Décret N° 2019-1036 du 8 octobre 2019 modifiant le 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 et les articles R. 1111-8-1 à R. 1111-8-7 du code de la santé publique
- 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
- HAS. Manuel de certification des établissements de santé pour la qualité des soins. Septembre 2021
- Critère 2.3-01 Les équipes respectent les bonnes pratiques d'identification du patient à toutes les étapes de sa prise en charge.
  - HAS. Amélioration des pratiques et sécurité des soins, la sécurité des usagers. Mettre en œuvre la gestion des risques associés aux soins en ES. Des concepts à la pratique Guide de gestion des risques. Mars 2012
  - Règlement européen «eIADS» n°910/2014 du 23 juillet 2014
  - Art. R. 1112-3 du CSP.
- Politique et organisation régionale de l'identitovigilance en région PACA