

	Document de consultation	Référence en nov	Date d'application	Version
		IDEN-DCO-0001	24/02/2022	005
Responsable(s) du document : Frédérique BOYER Service : Instances-comités\Identitovigilance				Pagination 1/10

Politique d'Identito-vigilance à l'Institut Bergonié

1 INTRODUCTION

La présente charte d'identitovigilance a pour objet de formaliser la politique conduite par l'Institut Bergonié 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 de l'établissement. Elle traite également des droits et devoirs des usagers qui sont également pleinement parties prenantes de leur propre sécurité.

2 POLITIQUE D'IDENTITOVIGILANCE

2.1 Définition et objectif

La maîtrise de l'identification des usagers est un enjeu majeur pour garantir la qualité et la sécurité de leur prise en charge, notamment lors des actes de soins – qu'ils soient réalisés à titre préventif, diagnostique ou curatif. L'identitovigilance représente l'ensemble des moyens organisationnels et techniques mis en œuvre pour disposer d'une identification unique, fiable et partagée du patient 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 du patient, dans le respect du secret médical.

2.2 Engagement de la structure

La direction de l'Institut Bergonié, en association avec les instances responsables de la qualité des soins et de la sécurité des usagers, entend conduire une politique d'identitovigilance conforme aux préconisations du Référentiel national d'identitovigilance (RNIV). Les objectifs poursuivis sont de :

- fiabiliser l'identification de chaque usager et des documents qui le concernent, à toutes les étapes de sa prise en charge ;
- utiliser l'identité INS (*identifiant national de santé*) conformément à la réglementation en vigueur;
- sécuriser les échanges d'informations personnelles de santé avec les correspondants extérieurs, dans le respect des droits du patient ;
- sensibiliser les différents acteurs – internes et externes à la structure – impliqués dans ces démarches.

Cette politique est définie en conformité avec les règles de bonnes pratiques établies dans le RNIV.

Les règles et grands principes d'identitovigilance appliquées à l'Institut figurent dans [IDEN-DCO-0002](#)

2.3 Structuration

La définition des procédures d'identitovigilance et leur mise en œuvre par les professionnels de l'Institut Bergonié, repose sur la cellule d'identitovigilance et les référents logiciels.

2.3.1 Le référent en identitovigilance

Le responsable de la cellule d'identitovigilance est désigné comme *référent en identitovigilance* pour l'Institut Bergonié. Il est identifié comme interlocuteur privilégié auprès de la cellule régionale d'identitovigilance.

Il est chargé, à ce titre, de :

- assurer la veille réglementaire et technique ;
- aider au repérage et à la gestion des risques liés à l'identification des usagers, en lien avec les autres vigilances et la DQGDR ;
- veiller à la promotion des bonnes pratiques dans son domaine, notamment par le biais de formations internes aux nouveaux arrivants et par la formation continue de l'ensemble des professionnels ;
- informer sans délai la direction des difficultés rencontrées en matière d'identitovigilance susceptibles de nuire à la sécurité des usagers ;
- participer à l'animation régionale par le biais de son adhésion au *réseau régional des référents en identitovigilance*.

2.3.2 La cellule d'identitovigilance (CIV)

La CIV est l'instance opérationnelle de l'identitovigilance de l'établissement. Elle a pour mission de participer, en lien avec la cellule QGDR, aux actions suivantes :

- sensibiliser l'ensemble des parties prenantes (professionnels, usagers) ;
- participer à la formation initiale et continue des professionnels amenés à créer ou modifier les identités dans le système d'information ;
- rédiger et/ou actualiser les procédures d'identitovigilance ;
- recueillir et analyser les événements indésirables en lien avec l'identitovigilance ;
- contrôler la qualité des bases de données utilisées par la structure ;
- recueillir et analyser les indicateurs qualité ;
- mettre en place les actions préventives et/ou correctives souhaitables.
- La CIV comprend les personnes référentes suivantes :
 - le responsable de la CIV, assurant la fonction de référent local en identitovigilance
 - le responsable de l'accueil et de la facturation
 - un représentant de la DSI
 - un cadre de la direction qualité gestion des risques
 - le coordonnateur de la gestion des risques associés aux soins
 - le médecin DIM
 - la directrice des systèmes d'information
 - la responsable intégration développement des systèmes d'information

- un cadre de santé
- l'administrateur des logiciels d'imagerie médicale

La liste actualisée des membres de la CIV est disponible dans la GED : [IDEN-EQ-0001](#)

La CIV se réunit au moins trois fois par an. Elle formalise un bilan périodique de ses activités, au moins annuel, qui précise les indicateurs suivis et leurs résultats, les incidents relevés et les mesures correctrices prises.

La CIV est chargée, sous l'autorité du référent en identitovigilance, de vérifier la mise en application des actions et de leur efficacité, en relation avec la Direction Qualité Gestion Des Risques (DQGDR). Les indicateurs suivis, les objectifs à atteindre et les actions planifiées dans le PAQSS sont formalisés dans le rapport annuel de la CIV.

2.3.3 Correspondants externes en identitovigilance externe

Les structures partenaires (ex : EFS) sont invités à identifier des correspondants en identitovigilance et transmettre leurs coordonnées à la CIV. Ils ont pour objet de faciliter la mise en commun des règles d'identitovigilance mais aussi de participer au signalement et au traitement des erreurs dans le cadre des données de santé échangées (domaine de rapprochement, cf. 3.3).

Ces correspondants peuvent être invités le cas échéant à participer aux réunions et actions de la « CIV » pour les sujets qui les concernent.

2.3.4 Référents logiciels

Le système d'information de l'Institut réunit plusieurs applications informatiques dédiées à des tâches spécifiques. Pour assurer la cohérence de l'ensemble des logiciels destinés à traiter des informations personnelles d'utilisateurs, chaque application est pilotée par un référent logiciel.

Il est le correspondant de la CIV pour tout ce qui concerne l'application des consignes d'identitovigilance dans son domaine. Son rôle est notamment d'assurer la cohérence des données avec le référentiel d'identités Hexagone, notamment lors des opérations liées au traitement des doublons ou erreurs d'identités.

La liste des applications informatiques partageant des données de santé nominatives et donc intégrées au domaine d'identification de la structure est tenue à jour par la directrice des systèmes d'information (DSI).

Les différents référents logiciels s'assurent de la qualité des flux de transmission des données d'identification et de leur bonne intégration dans les services clients.

2.4 Périmètre

La politique d'identitovigilance concerne l'ensemble des applications gérées par l'Institut Bergonié qui permettent d'identifier les usagers au travers du référentiel d'identités Hexagone. La cellule d'identitovigilance s'assure que les autres domaines d'identification échangeant des données avec les applications de l'Institut disposent également d'une politique d'identitovigilance compatible avec celle de l'Institut Bergonié.

2.5 Respect du RGPD

La direction de l'Institut Bergonié a formalisé, sous l'autorité de son délégué à la protection des données (DPO), la documentation prévue par le Règlement général de protection des données (RGPD), y compris pour l'utilisation de ces données dans le cadre de l'utilisation des services régionaux.

Une information est présente dans le livret d'accueil de l'établissement et précise les principes de partage des données d'identification personnelles dans le cadre régional et les modalités mises en œuvre pour respecter les droits de l'utilisateur.

3 ELÉMENTS D'IDENTIFICATION

3.1 Terminologie

L'objet de ce chapitre est de rappeler la signification des termes techniques utilisés dans l'établissement dans le domaine de l'identification du patient.

3.1.1 Identification

Identifier une personne consiste à disposer des informations nécessaires et suffisantes pour ne pas confondre cette personne avec une autre. Il 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 le patient dans le système d'information. Ils concourent à la sécurité de sa prise en charge.

3.1.2 Identité et identifiant numériques

Identité numérique : représentation de l'identité d'une personne physique dans un système d'information. L'identité numérique est composée d'un ou plusieurs identifiant(s) numérique(s) et de traits d'identification.

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 INS (Identifiant National de Santé) : ensemble de traits constituant l'identité sanitaire officielle d'un usager de la santé, tels qu'ils sont enregistrés dans des bases nationales.

On distingue plusieurs catégories d'identifiants numériques:

- l'identifiant d'épisode patient (IEP) ou numéro de séjour qui est créé pour chaque événement relatif au séjour du patient ;
- l'identifiant permanent patient (IPP) qui est créé pour chaque nouveau patient non encore connu de l'établissement. Chaque patient a donc un IPP unique¹, constant dans le temps, auquel sont rattachés les identifiants de venue ;
- le matricule INS qui correspond au numéro d'inscription au registre de l'INSEE (NIR ou NIA) associé à l'identité INS.

3.1.3 Domaine d'identification et de rapprochement

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

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

¹ Dans le cas d'un même patient identifié sous 2 IPP différents dans un même domaine d'identification, on parle de doublon (cf. 3.1.5).

NB : le rapprochement entre 2 identités numériques est également possible au sein d'un même DI ; il correspond à la recherche et au traitement des doublons ; on parle alors de « fusion » des identités numériques en doublon en une seule.

3.1.4 Traits d'identification

Les traits d'identification sont les informations définies dans un système d'information comme constituants de l'identité numérique d'un patient.

En cohérence avec le RNIV, l'Institut Bergonié distingue 2 catégories de traits d'identification.

- Les **traits stricts** : ce sont les informations de référence qui caractérisent l'identité sanitaire officielle de l'utilisateur ; elles permettent de référencer les données de santé partagées et de fiabiliser les rapprochements d'identités numériques entre structures
- Les **traits complémentaires** : ce sont des données qui apportent d'autres informations utiles à la prise en charge de l'utilisateur.

3.1.5 3.1.5 Doublons, fusion, collisions

- Le **doublon d'identités numériques** : il correspond à l'identification d'une même personne sous 2 identifiants numériques différents (ou plus) 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 et aboutit à la mise à disposition d'informations incomplètes.
- La **fusion** correspond au traitement des doublons ; elle consiste à regrouper toutes les informations d'un même individu sous un identifiant numérique unique.
- La **collision** correspond au regroupement, **sous un même identifiant numérique**, d'informations issues de **2 usagers différents** ; cela peut résulter d'une fusion réalisée avec des critères insuffisants, d'une erreur de choix de dossier patient lors d'une venue ou être la conséquence de l'utilisation frauduleuse d'une identité par un autre individu. Ces situations de non-qualité sont particulièrement difficiles à corriger.

3.2 3.2 Traits d'identification

Conformément au RNIV, l'Institut Bergonié classe les traits d'identification qu'il utilise selon 2 catégories. La fiche technique [IDEN-FICO-0001](#) définit comment sont retenus et vérifiés ces différents traits.

3.2.1 Traits stricts

- Nom de naissance (nom de famille)
- Premier prénom de naissance
- Date de naissance
- Sexe
- Lieu de naissance (code INSEE)
- Matricule INS (s'il existe, avec son OID)

3.2.2 3.2.2 Traits complémentaires

- Nom utilisé (nom porté dans la vie courante)
- Prénom utilisé (prénom porté dans la vie courante)

Leur recueil est obligatoire si le nom utilisé dans la vie courante par le patient est différent du nom de naissance et de même si le prénom couramment utilisé est différent du 1er prénom de naissance

3.3 Domaines d'identification et de rapprochement

Plusieurs domaines d'identification coexistent au sein du système d'information hospitalier (SIH) de l'Institut Bergonié. Ils sont tous reliés au référentiel d'identité Hexagone qui est le référentiel d'identités numériques maître sur lequel se raccordent les principales applications utilisées dans l'établissement.

Le dossier patient informatisé (Hôpital Manager), comme d'autres logiciels (HMBLOC/ANESTHESIE (gestion du PTI), CHIMIO (circuit des chimiothérapie), ARIA (gestion de la radiothérapie), ...) sont des applications totalement dépendantes d'Hexagone en termes de gestion des identités numériques. Ils font donc partie du même domaine d'identification que ce dernier.

Cependant, ils possèdent aussi leur propre identifiant numérique rattaché à un autre domaine d'identification.

Ces domaines d'identification sont « rapprochés » de celui d'Hexagone afin de garantir la cohérence des informations lors du parcours de chaque patient au sein de l'Institut Bergonié. Les identités numériques sont échangées par le biais d'une interface (EAI) qui permet de connecter les applications entre elles.

Les rapprochements avec les partenaires extérieurs au l'Institut Bergonié se font également au travers d'une interface EAI.

Toutes les applications gérant des identités numériques font donc partie d'un même domaine de rapprochement (cf. 3.1.3). Les flux informatiques entre les différents domaines utilisent des normes d'interopérabilité permettant de garantir la qualité des échanges ; exemples : HL7, IHE PAM, HPRIM, DICOM...

C'est également dans Hexagone que sont gérés les numéros de séjour (IEP) et les mouvements du patient.

3.4 Confiance dans les identités gérées

Conformément au RNIV, l'Institut Bergonié met en œuvre des procédures permettant la gestion de l'état de confiance des identités.

Dans Hexagone, chaque identité numérique est associée à un des 4 statuts de confiance suivants :

- « Identité provisoire » : aucune procédure de vérification d'identité n'a été réalisée
- « Identité validée » : une procédure de vérification d'identité a été réalisé à partir d'une pièce d'identité conforme
- « Identité récupérée » : l'identité a été récupérée par le biais du téléservice INSi
- « Identité qualifiée » : une procédure de vérification d'identité a été réalisé à partir d'une pièce d'identité conforme et l'identité a été récupérée par le biais du téléservice INSi.

3.5 Identités particulières

3.5.1 Confidentialité

Hexagone et HM permettent de signaler une identité confidentielle.

3.5.2 Homonymie

Il n'y a pas d'alerte informatique possible. Une procédure interne ([IDEN-FITC-0003](#)) permet d'informer les services de la présence de 2 personnes homonymes et d'en prendre compte dans l'attribution des lits d'hospitalisation.

3.6 Gestion de l'identité INS

En conformité avec le RNIV, l'Institut Bergonié met en place les procédures de formation et d'authentification des professionnels autorisés à accéder au téléservice INSi pour la gestion des identités INS.

Des procédures ad hoc précisent les conditions dans lesquelles le téléservice INSi est appelé et la gestion des identités numériques qui en découle, soit en mode « recherche et récupération », soit en mode « vérification d'une identité INS ».

4 GESTION DES RISQUES A PRIORI

4.1 Gestion documentaire

L'Institut Bergonié dispose d'un système de gestion électronique documentaire (GED) via le logiciel ENNOV qui est géré par la DQGDR. Elle est chargée de la diffusion de l'information sur la publication de nouveaux documents.

Un portail dédié à l'identitovigilance intègre tous les documents relatifs à l'identitovigilance approuvés et validés par la cellule d'identitovigilance. Ils sont actualisés en tant que besoin et sont ainsi accessibles à l'ensemble des professionnels qui prennent en charge l'utilisateur, dans leur domaine de compétence.

Ce portail contient aussi :

- les comptes rendus de la cellule d'identitovigilance ;
- le lien internet vers le site d'identitovigilance de Nouvelle Aquitaine ;
- Des supports pédagogiques en lien avec les bonnes pratiques d'identitovigilance

4.2 Gestion des habilitations

Avant de pouvoir accéder au système d'information, une demande de création de compte doit être réalisée en amont de son arrivée par la Direction des ressources humaines (DRH) ou le cadre N+1. A son arrivée, tout nouvel arrivant doit préalablement signer la *charte utilisateur* du système d'information. Conformément à la politique de sécurité en vigueur, des droits d'accès plus ou moins étendus lui sont attribués en fonction de son profil métier et de ses missions.

L'agent récupère son *login* et mot de passe auprès de la Direction des systèmes d'information (DSI).

Les droits d'accès des professionnels partis de l'Institut sont supprimés dès connaissance de leur départ définitif.

Une revue annuelle des habilitations est réalisée, elle permet de vérifier et réactualiser la liste des professionnels et des droits attribués.

La direction des systèmes d'information tient à jour les matrices d'habilitation des différents logiciels.

4.3 Traçabilité des actions

L'ensemble des applications informatiques liées aux données de santé utilisées par l'Institut Bergonié possèdent un dispositif d'enregistrement horodaté des accès précisant le nom (*login*), le type d'accès (lecture ou écriture) et les pages visitées. En application de l'article R6113-9-2 du code de la santé publique, la traçabilité des actions (création, modification et consultation) sont conservées pendant au moins 6 mois.

L'accès à ces informations n'est autorisé qu'à un nombre réduit de professionnels (directeur, DSI, responsable de la CIV). Un contrôle peut être décidé lorsqu'il existe un doute sur le comportement d'un professionnel ou à titre systématique, par exemple pour vérifier l'absence d'intrusion externe dans le système d'information.

En termes d'identitovigilance, le système conserve pendant toute la durée de vie du dossier patient l'historique des modifications apportées sur les identités numériques, y compris les modifications apportées aux IPP.

4.4 Information des usagers

Le livret d'accueil du patient de l'Institut Bergonié intègre un chapitre concernant la gestion de l'identité patient et les droits d'accès et de modification à ses données. Il précise l'importance d'une identification fiable et la nécessité de disposer de documents permettant de confirmer l'identité.

Pour l'ensemble des usagers, des documents (flyers, affiches) permettent également de les informer sur les règles d'identitovigilance et les pratiques de vérification de l'identité tout au long de sa prise en charge, notamment avant chaque acte de soins. Ces supports sont disponibles dans tous les services et lieux d'accueil de l'Institut.

La conformité au RGPD fait également l'objet d'une information appropriée.

4.5 Formation et sensibilisation des acteurs

Un module de formation en e-learning est proposé à tout nouvel arrivant via le logiciel ENNOV.

Un quizz est à disposition de tous les professionnels sur le portail ENNOV :

« Tester vos connaissances sur l'identitovigilance, êtes-vous d'accord avec les 16 affirmations suivantes ? »

Le plan de formation continue intègre un module en lien avec l'identitovigilance, inclus dans la formation à la Qualité et Gestion des Risques (catalogue ATRIUM).

Lors de la semaine sécurité des patients, le thème identitovigilance est régulièrement abordé.

5 GESTION DES RISQUES A POSTERIORI

5.1 Gestion documentaire

On retrouve dans ENNOV les documents relatifs à la gestion des risques *a posteriori* en lien avec un dysfonctionnement relatif à l'identification d'un patient : déclaration des événements indésirables et le cas échéant réalisation d'enquêtes et retours d'expérience adaptés aux erreurs d'identitovigilance.

5.2 Déclaration et gestion des événements indésirables

L'Institut Bergonié a un processus de signalement des événements indésirables via ENNOV, piloté par la DQGDR. Il promeut son emploi par l'ensemble des professionnels de l'établissement en priorisant les événements indésirables

ayant un impact potentiel sur la sécurité des soins et notamment le signalement des erreurs en lien avec l'identification des patients.

Un bilan annuel des EI est réalisé et les EI en lien avec l'identitovigilance font l'objet d'un focus particulier.

La CIV, en association avec la DQQGR, organise des actions de formation et de sensibilisation sur l'importance et les modalités des signalements en rapport avec l'identitovigilance.

Dès qu'une fiche d'événement indésirable (FEI) en lien avec l'identitovigilance est renseignée, elle est envoyée pour traitement au destinataire qui pourra analyser et répondre à la problématique et la fiche est enregistrée en identitovigilance pour être présentée en cellule d'identitovigilance.

Lorsque les conséquences sont graves et que l'EI est éligible, le signalement des événements indésirables est réalisé sur le portail national de signalement des événements sanitaires indésirables. Afin de favoriser la reconnaissance et la prévention des sources d'erreurs en matière d'identification des usagers, l'ARS Nouvelle Aquitaine a mis en place une **Fiche de signalement d'événement indésirable en rapport avec une erreur d'identification** ([IDEN-DEXT-0001](#)) pour que lui soit signalée *a minima* toute erreur d'identification :

- en lien avec une obligation de signalement externe réglementaire ;
- entraînant la transmission d'une identité erronée à un ou plusieurs acteurs de santé externes à notre structure (même dans le cas où celle-ci a été corrigée rapidement) ;
- susceptible d'avoir des conséquences juridiques (réclamation, plainte...);
- jugée intéressante à partager au niveau régional, de façon anonymisée, pour améliorer la culture de sécurité.

En cas d'évènement indésirable en rapport avec une erreur d'identification, cette fiche dûment complétée est à adresser dans les meilleurs délais au *Point Focal Régional* de l'ARS par mail : ars33-alerte@ars.sante.fr ou par fax : [05.67.76.70.12](tel:05.67.76.70.12). Il est recommandé de mettre en copie l'adresse mail de la Cellule régionale d'identitovigilance (CRIV) : criv@esea-na.fr

5.3 Gestion d'une erreur d'identité

Toute fiche d'événement indésirable en lien avec une erreur d'identité est traitée sans délai. Les délais de mise en œuvre des actions proposées dépendent de la nature de l'évènement. La revue des EI en cellule d'identitovigilance permet un suivi des actions engagées.

Les informations issues des déclarations d'EI enrichissent une base de données tenue par la CIV. Elle sert à la formation et à la sensibilisation des professionnels ainsi qu'à la mise à jour régulière des indicateurs de suivi.

5.4 Gestion des anomalies du domaine de rapprochement

La CIV est chargée de s'assurer régulièrement de la qualité de la base de données des identités de chaque domaine d'identification mis en œuvre par l'Institut Bergonié. Des procédures et modes opératoires, consultables dans ENNOV précisent les responsabilités et modalités d'organisation des opérations d'évaluation et de corrections à mettre en œuvre en cas de doublons, collisions, ...

Une adresse mail est dédiée aux demandes de correction (doublons et collisions) : A- Doublons-Identite-Patients

5.5 Indicateurs de suivi

La CIV suit un certain nombre d'indicateurs dans le domaine de l'identitovigilance qui ont pour objet de caractériser et de quantifier les problèmes de sécurité en lien avec l'identité des patients. Ils sont analysés à chaque réunion de l'instance et font l'objet, si nécessaire, de propositions d'actions d'amélioration. Les actions retenues sont enregistrées, priorisées en fonction de leur niveau de criticité et font l'objet d'une évaluation afin de vérifier l'efficacité de leur mise en œuvre.

Principaux indicateurs suivis par la CIV :

- Nombre dossiers fusionnés
- Taux ou nombre de formation des professionnels à l'identitovigilance
- Nombre de réunions annuelles de la CIV

6 UTILISATION DE SERVICES D'E-SANTÉ RÉGIONAUX

L'Institut Bergonié utilise certains services d'échange et de partage de données de santé mis à disposition au niveau régional pour améliorer les parcours de santé.

Les modalités d'interfaçage à chaque service et les règles relatives aux transferts de données font l'objet d'une convention d'engagement mutuel signée avec le porteur de la solution.

Afin de garantir le respect des termes de la convention, l'Institut Bergonié confie à chaque référent logiciel concerné par l'utilisation d'un service la mission de s'assurer de la conformité des échanges de données numériques entre le logiciel et l'application régionale utilisée par rapport aux exigences techniques et réglementaires applicables.

Il est notamment en charge de la mise en œuvre effective d'une procédure d'alerte réciproque entre l'Institut Bergonié et :

- le porteur de la solution en cas d'événement indésirable relatif aux problèmes d'interopérabilité ;
- la cellule régionale d'identitovigilance (CRIV) si l'événement indésirable est associé à l'identification de l'utilisateur ou à la diffusion erronée d'une identité INS incorrecte ;

Des procédures ad hoc sont formalisées, en lien avec le référent local en identitovigilance, et consultables dans la GED. Les erreurs d'identification peuvent également justifier un signalement externe.

La communication de l'utilisation de ces services aux usagers est assurée par l'intermédiaire de plusieurs vecteurs.

7 RÉFÉRENCES RÉGLEMENTAIRES ET TECHNIQUES

Référentiel national d'identitovigilance (RNIV) _Juin 2021

Guide méthodologique de mise en œuvre de l'identité patient au sein des groupements hospitaliers de territoire (ASIP Santé, 2018)

Modèle régional de charte d'identitovigilance des établissements sanitaires et médico-sociaux (V2-décembre 2020)