CHARTE D'IDENTITOVIGILANCE

SOMMAIRE

La structure générale d'une charte d'identitovigilance locale, illustrée dans les chapitres du présent document, est la suivante (sans parler de la page de garde avec le nom de la structure, l'intitulé du document des éléments de version et de validation du document dans le système documentaire) :

1 INTRODUCTION

La présente charte d'identitovigilance a pour objet de formaliser la politique conduite par la Maison de Santé Béthel pour bien identifier les patients/résidents 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 patients/résidents 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 patients/résidents 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 patients/résidents. 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.

Une procédure interne décrit l'organisation de l'identitovigilance au sein de l'établissement (PC-GR 009).

2.2 Engagement de la structure

La direction de l'établissement, en association avec les instances de la CQGR et la CIV, 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 patient/usage 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.

Ces objectifs intègrent la politique d'identitovigilance décrite dans le guide des politiques de la Maison de Santé Béthel (DV-SQ 025).

2.3 Gouvernance

La définition des procédures d'identitovigilance et leur mise en œuvre par les professionnels de l'établissement, repose sur une organisation spécifique qui comprend :

- le correspondant identitovigilance ;
- la cellule d'identitovigilance (CIV) qui assure également le pilotage de l'identitovigilance ;
- les référents logiciels.

2.3.1 Le comité de pilotage de l'identitovigilance :

Le comité de pilotage n'est pas identifié en tant que tel mais est assuré par la CIV, et intègre ses missions. Il a pour objet de définir les orientations de la politique d'identitovigilance et les moyens à mettre en œuvre pour la faire respecter, en conformité avec les principes établis par le RNIV. Il s'assure de la mise à jour et de la cohérence des différentes applications du système d'information, valide les documents publiés par la structure dans ce domaine. Il se tient informé des résultats obtenus et des difficultés rencontrées. Il contrôle la cohérence du plan de formation avec les objectifs de formation et de sensibilisation des différents acteurs concernés.

La CIV se réunit une fois par an pour définir le pilotage, de préférence en début d'année afin de faire le bilan de l'année précédente et de définir les objectifs de l'année en cours.
Lors de cette réunion exceptionnelle de la CIV, sont invités en plus des membres :

- le directeur ;
- la directrice des soins ;
- le président de la commission médicale d'établissement (CME) ;
- le responsable de la sécurité des systèmes d'information (RSSI) ;
- le délégué à la protection des données (DPD) rattaché à l'établissement.

2.3.2 Le correspondant identitovigilance

Le président de la cellule d'identitovigilance (CIV) est désigné comme correspondant identitovigilance pour l'établissement. Il est chargé, à ce titre, de :

- Représenter la CIV de la commission qualité et gestion des risques (CQGR) ;
- Assurer la veille réglementaire et technique ;
- Aider au repérage et à la gestion des risques liés à l'identification des patients/résidents, en lien avec les autres vigilances et la CQGR ;
- 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 professionnels ;
- Informer la CIV 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.

2.3.3 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 CQGR, aux actions suivantes :

- Sensibiliser l'ensemble des parties prenantes (professionnels, patients/résidents) ;
- 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 évènements 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 président de la CIV, assurant la fonction de correspondant identitovigilance et de gestionnaire des risques associés aux soins;
- le responsable de l'accueil et de la facturation ou son représentant ;
- le responsable qualité ;
- un cadre de santé ;
- des référents d'identitovigilance ;
- des référents logiciels ;
- un représentant des usagers, sur invitation.

La liste actualisée des membres de la CIV (EN-AF 001n) est disponible dans le logiciel qualité et gestion des risques.

La CIV se réunit au moins quatre fois par an. Elle formalise un bilan annuel de ses activités qui précise les indicateurs suivis et leurs résultats, les incidents relevés et les mesures correctrices prises. Ce bilan est communiqué à la direction et aux professionnels de l'établissement. Il en est de même pour les procès-verbaux des réunions.

La CIV est chargée, sous l'autorité du correspondant identitovigilance, de vérifier la mise en application des actions et de leur efficacité, en relation avec la CQGR. Les indicateurs suivis, les objectifs à atteindre et les actions planifiées dans le PAQ sont formalisés dans le rapport annuel de la CIV.

2.3.4 Référents et correspondants en identitovigilance

- **Référents en identitovigilance internes**

  Un référent en identitovigilance est désigné dans chaque secteur de soins. Ce professionnel a pour mission d'assurer le relais des décisions de la CIV dans les différents secteurs d'activité. Il est également chargé de faire remonter les difficultés rencontrées par les acteurs de terrain.

  Il participe aux actions de formation et de sensibilisation en matière d'identitovigilance et est membres de la CIV.

- **Correspondants en identitovigilance externes**

  Les structures partenaires (laboratoire de biologie Bio67, établissement français de sang (EFS)) sont invitées à identifier des correspondants en identitovigilance et à transmettre leurs coordonnées à la CIV de l'établissement. 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.

  Selon les besoins, ces correspondants externes sont invités à participer aux réunions et actions de la CIV pour les sujets qui les concernent.

2.3.5 Référents logiciels

Le système d'information de la structure 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'usagers, chaque application est pilotée par un référent logiciel. Ils sont définis dans le protocole « Conduite à tenir en cas de panne d'un des logiciels » (PT-GR 033), mis à disposition de l'ensemble des responsables de l'établissement.

La liste des applications informatiques partageant des données de santé nominatives et donc intégrées au domaine d'identification de la structure (DV-SI 036) est tenue à jour par le responsable de la sécurité des systèmes d'information (RSSI).

2.4 Périmètre

La politique d'identitovigilance concerne l'ensemble des applications gérées par l'établissement qui permettent d'identifier les usagers.

2.5 Respect du RGPD

La direction de l'établissement 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.

Un document d'information sur l'utilisation de ces services est présenté dans le livret d'accueil de l'établissement.

3 ÉLEMENTS 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/résident.

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/résident 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.

Au sein de l'établissement, il est distingué plusieurs catégories d'identifiants numériques :

- *L'identifiant d'épisode patient* (IEP) qui est créé pour chaque événement relatif au séjour du patient : c'est le numéro de séjour/hospitalisation ;
- *L'identifiant permanent patient* (IPP) qui est créé pour chaque nouveau patient/résident non encore connu de l'établissement. Chaque patient/résident a donc un IPP unique
- 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/résident est représenté par un seul IPP. Chaque DI identifie le patient/résident 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 ».

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/résident. Exemple de traits : nom, prénom, date de naissance, sexe.

En cohérence avec le RNIV, l'établissement distingue 2 catégories de traits d'identification (cf. 3.2).

- Les **traits stricts** : ce sont les informations de référence qui caractérisent l'identité sanitaire 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 complémentaires** : ce sont des données qui apportent d'autres informations utiles à la prise en charge de l'usager.

3.1.5 Doublons, fusion, collisions

Les termes employés en identitovigilance sont définis dans l'annexe II du volet socle du RNIV (*1. 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.

- 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 Traits d'identification

Conformément au RNIV, l'établissement classe les traits d'identification qu'il utilise selon 2 catégories. Une procédure interne définit comment sont retenus et vérifiés ces différents traits (« Généralités et précisions sur la création d'identité du patient » PT-GR 019).

3.2.1 Traits stricts

- *Nom de naissance* ;
- *Premier prénom* d'état civil ;
- *Liste des prénoms* de naissance figurant sur un titre officiel d'identité ;
- *Date de naissance* ;
- *Sexe* ;
- *Lieu de naissance*, sous forme de code INSEE de la commune (pour les usagers nés en France) ou du pays (pour les autres) ;
- *Matricule INS* (toujours associé à son OID : identifiant numérique spécifique associé au matricule INS qui permet de distinguer sa nature : NIR).

3.2.2 Traits complémentaires

- *Nom utilisé* : nom de naissance, nom d'usage lié à un acte d'état civil ;
- *Prénom utilisé* : premier prénom de l'état civil ;
- *Code postal* de la commune de naissance (pour les usagers nés en France exclusivement) ;
- *Commune de naissance* ;
- *Identifiant patient permanent* (IPP) ;
- *Adresse de résidence* de l'usager ou de l'assuré ;
- Numéros de téléphone (portable et fixe) ;
- Adresse(s) courriel de contact ;
- Nom des personnes en relation (parents, enfant, conjoint, personne de confiance…) ;
- Nom et coordonnées de la personne de confiance ;
- Nom et coordonnées du médecin traitant ;
- Autres professionnels de santé impliqués dans la prise en charge ;
- Profession ;
- Type de document d'identité présenté.

3.3 Domaines d'identification et de rapprochement

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

Le dossier patient informatisé (« Cariatides»), qui est une application totalement dépendante en termes de gestion des identités numériques.

D'autres logiciels, qui utilisent une base de données d'identités numériques propres, constituent des domaines d'identification distincts. Pour exemples :

- « HESTIA » (Gestion de l'hôtellerie).
- « CEGI » (Gestion administrative patient).

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

Les rapprochements avec les partenaires extérieurs à l'établissement se font également au travers d'une interface.

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

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

3.4 Confiance dans les identités gérées

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

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

- « Identité provisoire » ;
- « Identité validée » ;
- « Identité récupérée » ;
- « Identité qualifiée ».

Les modalités pratiques d'attribution et de gestion de ces statuts sont précisées dans la procédure générale de recueil de l'identité, disponible dans la gestion documentaire.

3.5 Identités particulières

Le logiciel assure la confidentialité relative aux prises en charge effectuées dans l'établissement. Bien qu'il soit exceptionnellement confronté à des demandes d'usagers destinées à accroître cette confidentialité (anonymat, situations nécessitant la gestion d'identités sensibles…), l'établissement dispose d'un protocole précisant la conduite à tenir face à une exigence particulière en termes d'identification, dans le respect de la réglementation en vigueur.

3.6 Gestion de l'identité INS

En conformité avec le RNIV, l'établissement s'assure de la formation et de l'authentification des professionnels autorisés à accéder au téléservice INSi pour la gestion des identités INS.

4 GESTION DES RISQUES *A PRIORI*

4.1 Gestion documentaire

L'établissement dispose d'un système de gestion électronique documentaire (GED) qui est géré par le service qualité pour la partie qui concerne les documents qualité. Le service, après validation des personnes concernées, est chargé de la diffusion de l'information aux professionnels concernés.

La GED intègre tous les documents relatifs à l'identitovigilance approuvés par la CIV et validés par la direction Ils sont actualisés en tant que besoin et sont accessibles à l'ensemble des professionnels qui prennent en charge l'usager, dans leur domaine de compétence.

Les documents en rapport avec l'identitovigilance comprennent :

- la présente charte d'identitovigilance ;
- les comptes rendus des instances (CIV…) ;
- les protocoles et les procédures en vigueur dans la structure ;
- les recommandations et bonnes pratiques publiées par des sociétés savantes.

4.2 Gestion des habilitations

Avant de pouvoir accéder au système d'information, tout nouvel employé doit préalablement signer la charte informatique (DV-SI 009). 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, tels qu'ils sont décrits dans la matrice des droits (DV-DP 003).

Le professionnel récupère son login et mot de passe auprès du service informatique. Ils lui sont remis contre émargement.

Toute sortie définitive de l'établissement est signalée au service informatique par le service ressources humaines dans la semaine afin de supprimer les droits d'accès de la personne.

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

Le service informatique tient à jour un certain nombre de documents qui sont actualisés en fonction des besoins :

- La matrice des droits ouverts en fonction de la qualification des professionnels ;
- La liste des professionnels disposant de codes d'accès actifs précisant la date de début des droits et, pour ceux qui ont quitté définitivement la structure, de fin des droits.

4.3 Traçabilité des actions

L'ensemble des applications informatiques liées aux données de santé utilisées par l'établissement 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, service informatique, 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. Les modalités d'accès sont précisées dans une procédure *ad hoc* consultable sur la GED.

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 (fusion de dossiers).

4.4 Information des usagers

Le livret d'accueil du patient de l'établissement 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. Des informations sont également communiquées sur les écrans d'information mis en place aux admissions.

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 leur prise en charge, notamment avant chaque acte de soins.

La conformité au RGPD fait également l'objet d'une information appropriée (« Notice d'information du patient » (DV-GR 044)).

4.5 Formation et sensibilisation des acteurs

La politique d'identitovigilance et les bonnes pratiques en identitovigilance sont reprises dans le livret d'accueil du personnel.

Le plan de formation continue intègre des formations en lien avec l'identitovigilance.

Lors de la semaine sécurité des patients, le thème identitovigilance peut être abordé, il est mis en place des ateliers à destination des professionnels et des usagers.

5 GESTION DES RISQUES A POSTERIORI

5.1 Gestion documentaire

On retrouve dans la gestion documentaire les documents relatifs à la gestion des risques *a posteriori*, c'est-à-dire aux actions à mettre en œuvre après la mise en évidence d'un dysfonctionnement relatif à l'identification d'un patient : déclaration des événements indésirables, réalisation des enquêtes et des retours d'expérience adaptés aux erreurs d'identitovigilance…

5.2 Déclaration et gestion des événements indésirables

L'établissement met en œuvre un système de signalement des événements indésirables (FEI). 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.

La structure communique également auprès de ses partenaires (laboratoire, EFS, médecins et autres professionnels de santé extérieurs) pour qu'ils lui signalent les anomalies constatées sur l'identification des patients.

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

Toute fiche d'événement indésirable (FEI) en lien avec l'identitovigilance est traitée lors d'une réunion de la CIV. Selon la gravité et le risque, des actions correctives ont été mises en place avant la réunion.

Lorsque les conséquences sont graves, le signalement des événements indésirables est réalisé selon les consignes applicables, soit par le biais du portail national de signalement des événements sanitaires indésirables – lorsque l'EI est éligible – soit directement à l'ARS (cf protocole « Que faire en cas d'EIG ou EIGS » ? (PT-GR 036)).

5.3 Gestion d'une erreur d'identité

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

En cohérence avec le RNIV, la « CIV » s'engage à définir la conduite à tenir face à l'identification d'une erreur et à identifier les actions correctives à mettre en œuvre, selon la situation.

Ces informations 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

Des procédures et modes opératoires, consultables dans la GED (cf. 4.1) précisent les responsabilités et modalités d'organisation des opérations d'évaluation et de corrections à mettre en œuvre :

- Identification et gestion des doublons (PT-GR 027) ;
- Identification et gestion des collisions (PT-GR 027) ;
- Transmission des informations relatives à ces corrections aux autres domaines d'identité et professionnels concernés.

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 en réunion de l'instance et font l'objet, si nécessaire, de propositions d'actions d'amélioration. Les actions retenues sont intégrées dans le PAQ de l'établissement.

Quelques indicateurs suivis par la CIV :

- Taux d'erreur d'identité dans l'établissement ;
- Taux de doublon de dossier ;
- Pourcentage de demandes d'autorisation du nom sur la porte de la chambre pour les patients du SSR, de l'USLD et de l'UVS ;
- Evaluation de l'utilisation du bracelet d'identification.

6 UTILISATION DE SERVICES D'E-SANTE REGIONAUX

L'établissement 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'établissement 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.

Les erreurs d'identification peuvent justifier un signalement externe.

La communication de l'utilisation de ces services aux usagers est assurée par l'intermédiaire du livret d'accueil.

7 REFERENCES REGLEMENTAIRES ET TECHNIQUES

- Référentiel national d'identitovigilance (RNIV)
- Manuel de certification de la HAS et référentiel d'évaluation des ESSMS de la HAS
- Charte régionale d'identitovigilance Grand Est (Pulsy)