GRIVES

Groupe Régional d'Identitovigilance des Etablissements de Santé

CHARTE D'IDENTITOVIGILANCE

Indiquer ici le nom de votre structure

Objet du document

Le GRIVES vous propose un modèle de charte locale/territoriale d'identitovigilance respectant les exigences et recommandations du Référentiel national d'Identitovigilance (RNIV).

Type de document	MODELE	Charte locale/territoriale d'identitovigilance	
Version	V1	Date	29/06/2021
Périodicité de révision	Triennale	Lors d'évolutions réglementaires	Lors d'évolution des pratiques

SOMMAIRE

PRESENTATION ET MODE D'EMPLOI DU DOCUMENT

A la demande de nombreux établissements, le GRIVES vous propose un modèle de charte locale/territoriale ou de groupement d'identitovigilance conforme aux exigences du Référentiel national d'identitovigilance (RNIV) et au référentiel INS.

Ce modèle a pour vocation d'évoluer dans le temps en fonction des nouvelles réglementations et pratiques. Le GRIVES assurera une veille dans ce domaine et apportera les corrections nécessaires au document.
Toute suggestion ou demande de modification peut être adressée au GRIVES (grives@ies-sud.fr).

Les indications *en bleu italique* sont destinées à apporter une aide à la rédaction, ou des conseils à l'établissement et doivent être supprimées une fois la charte de la structure rédigée.
Les termes en *vert italique* concernent les établissements partie ou associés à un GHT ou à un groupement de structures privées. Ils doivent être supprimés si la structure ne fait pas partie d'un GHT ou d'un groupement.
Les acteurs mentionnés en *italique rouge* dans le texte ne sont pas imposés par le RNIV. Ils sont recommandés en région PACA.

Il est conseillé aux structures de suivre le plan proposé afin de balayer l'ensemble de la thématique identitovigilance dans la charte.

Si ce document doit être imprimé, il est conseillé de réaliser une impression couleur afin de bien distinguer les aides à la rédaction.

INTRODUCTION

Objet du chapitre : décrire les objectifs de la charte d'identitovigilance.
Exemple de rédaction :

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.

La charte d'identitovigilance a pour objet de formaliser la politique conduite par *indiquer ici le nom de votre structure* 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.

Cette charte est révisée :
- tous les 3 ans ;
- en cas d'évolution réglementaires ;
- en cas d'évolutions des pratiques, du contexte locale, des organisations…

POLITIQUE D'IDENTITOVIGILANCE

Le GRIVES vous propose une politique générique pour alimenter votre réflexion. Les éléments doivent être adaptés aux problématiques et à la stratégie de la structure, sa patientèle, son projet d'établissement, son projet qualité, les évènements indésirables rencontrés dans la structure…

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 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.

Le *CH mettre ici le nom de la structure* 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.
La politique d'identitovigilance est élaborée par la direction en concertation avec les instances responsables de la qualité des soins et de la sécurité des usagers, en concertation avec les représentants d'usagers. Son élaboration tient compte des objectifs stratégiques de l'établissement en termes de qualité et de sécurité des soins, des caractéristiques des risques identifiés dans l'établissements (activité à risques, usagers à risques…)

La politique d'identitovigilance du *CH mettre ici le nom de la structure* a pour objectif :

- d'améliorer la qualité et la sécurité des prises en charge ;
- de favoriser le respect des bonnes pratiques d'identification des par les professionnels en renforçant la culture qualité sécurité des soins de tous les professionnels en matière d'identification des usagers ;
- de déployer l'INS et ses usages dans l'établissement et pour les échanges avec les professionnels participant à la prise en charge de l'usager (alimentation du Dossier Médical Partagé -DMP, transmission par Messagerie sécurisée de Santé - MSsanté de documents référencés avec l'INS…) ;
- de mettre en conformité son organisation et ses pratiques avec le RNIV afin de garantir la sécurité de l'utilisation de l'INS ;
- de réduire le risque d'erreur sur l'identification de la personne prise en charge ;
- de réduire le risque d'erreurs liées à l'identification secondaire des usagers en particulier au niveau de l'imagerie médicale, de la réalisation de prélèvements biologiques, du processus de prise en charge médicamenteuse, des blocs opératoires, du processus transports intra hospitaliers (*les activités mentionnées ici sont identifiées comme étant les plus à risques, l'établissement adapte si nécessaire les activités listées*) ;
- de contribuer à l'unicité du dossier de l'usager c'est-à-dire d'assurer qu'une identité, et une seule, correspond à chaque personne physique prise en charge au sein de l'établissement, quelle que soit cette prise en charge et de permettre ainsi l'accès à l'ensemble des informations concernant un usager, en minimisant le risque de méconnaître une partie des données ;
- de sécuriser les échanges d'informations personnelles de santé avec les correspondants extérieurs, dans le respect des droits de l'usager ;
- de contribuer à améliorer l'interopérabilité des systèmes d'information au sein de l'établissement, en respectant les normes d'interopérabilité, en testant chaque fois que nécessaires les interfaces, en impliquant les professionnels utilisateurs…

Si l'établissement est membre d'un groupement ou d'un GHT, penser à enrichir les objectifs dans le cadre de la convergence, par exemple :

- *sécuriser les projets de convergence des identités dans le cadre de la mise en place d'un dossier patient informatisé de groupement…*
- *sécuriser les échanges inter-établissement…*

Cette politique est définie en conformité avec les règles de bonnes pratiques établies par le RNIV (volets 0 et 2 spécifique des établissements de santé, volet 3 pour les établissements éligibles).

Afin de conduire cette politique ambitieuse d'identitovigilance, l'établissement a défini et mis en place les moyens humains et matériels nécessaires (cf. gouvernance de l'identitovigilance). *Si des moyens matériels ont été spécifiquement mis en place pour améliorer l'identitovigilance (exemple acquisition d'un logiciel spécifique de dépistage des anomalies, de signalement…), vous pouvez les mettre en valeur ici.*

1. Périmètre d'application de la politique

a) Mode de prise en charge

La politique d'identification de l'usager s'applique à tous les modes de prise en charge présents proposés par le *CH indiquer ici le nom de la structure* :
Décrire ici les modes de prises en charges :
- *hospitalisations, conventionnelles ou ambulatoires ;*
- *consultations externes, programmées ou en urgence, en présentiel ou à distance (télémédecine);*
- *séances… ;*
- *EHPAD et médico-social.*

b) 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 ou secondaire) :

Citer ci-dessous la liste des professionnels participant à l'identification de l'usager
- *les médecins et le personnel paramédical (aide-soignant, infirmiers, sage femmes, auxiliaires puéricultrices…) ;*
- *les secrétaires médicales ;*
- *les brancardiers ;*
- *les personnels médicaux, para médicaux et médico-techniques des services médico-techniques :*
  - *laboratoire ;*
  - *imagerie ;*
  - *pharmacie à usage intérieur ;*
  - *plateau technique de rééducation fonctionnelle ;*
  - *unité transversale de diététique ;*
  - *centre d'exploration fonctionnelle ;*
  - *…*
- *les personnels administratifs réalisant l'identification des usagers ou traitant son dossier y compris la prise de rendez-vous, physique, électronique ou téléphonique*
  - *bureau des entrées ;*
  - *secrétariats médicaux ;*
  - *service des archives ;*
- *les personnels des services informatiques ;*
- *les intervenants de sociétés tierces réalisant des prises de rendez-vous par téléphone ;*
- *les personnels des départements d'information médicale (MIM – TIM …).*
- *Les professionnels de santé libéraux associés à une démarche d'échange et partage ville hôpital ;*
- *Les professionnels du secteur médico-social associés à une démarche d'échange et partage ville hôpital.*

c) Système d'information

La politique d'identitovigilance concerne l'ensemble des applications présentes dans le *CH indiquer ici le nom de la structure* qui participe à l'identification de l'usager, qu'elles soient ou non alimentées par le référentiel d'identité (cf. cartographie applicative). 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 le responsable des systèmes d'information (RSI).

Vous pouvez, si vous le souhaitez préciser les applicatifs mais il est conseillé de renvoyer à la cartographie applicative pour éviter d'avoir plusieurs documents contenant les mêmes informations. Inclure tous les outils contenant des identités patients (les logiciels de gestion des repas et des régimes, les outils de reconnaissance et de dictée vocale font appel à des identités patients et doivent être considérés comme participant à la prise en charge).

GOUVERNANCE DE L'IDENTITOVIGILANCE

Objet du chapitre : préciser la structuration de l'identitovigilance dans la structure :

L'identitovigilance au sein du *CH indiquer ici le nom de la structure* repose sur une organisation spécifique qui comprend :
- le comité stratégique en identitovigilance ;
- le référent en identitovigilance ;
- la cellule opérationnelle d'identitovigilance ;
- *les correspondants en identitovigilance des services cliniques et médico-techniques ;*
- les référents logiciels.

Il est possible de proposer un organigramme fonctionnel et/ou hiérarchique pour décrire l'organisation de l'identitovigilance dans la structure. Si cela est le cas, rajouter la phrase : l'organisation de l'identitovigilance est décrite dans l'organigramme fonctionnel et/ou hiérarchique (mettre ici la référence de l'organigramme dans la gestion documentaire).

Les éléments de gouvernance proposés ci-dessous sont destinés aux instances locales. Ils peuvent être adaptés pour convenir aux instances territoriales (groupements hospitaliers de territoire ou groupements de structure privées). Une proposition de gouvernance pour les groupements et les GHT est présentée en annexe 1.

Pour les établissements sanitaires de petite taille, n'exerçant pas d'activité à haut risque et qui ont obtenu l'accord de l'ARS pour appliquer le RNIV 3 (cf. fiche pratique FIP 13 «Aide à la décision en vue d'autoriser les ES à appliquer le RNIV3» proposée par le réseau des référents régionaux en identitovigilance ou 3RIV), une proposition de gouvernance est présentée en annexe 2. Il est nécessaire dans ces structures d'identifier un comité d'identitovigilance et d'un référent en identitovigilance. Le comité d'identitovigilance exerce alors les missions stratégiques et opérationnelles.

1. Le comité stratégique en identitovigilance (« COSTRATIV »)

Objet du chapitre : préciser la dénomination, le rôle et la composition du niveau décisionnaire. Il est fortement conseillé de ne pas identifier les membres nominativement dans la charte et de prévoir annuellement une note de désignation nominative (ceci permet de ne pas devoir revoir la charte à chaque changement d'un membre).

a) Composition

La structure ne conserve que les membres pertinents au regard de son activité. La structure peut compléter la composition du COSTRATIV.
Point d'attention : il est important que les soignants soient représentés dans l'instance stratégique.

La composition du COSTRATIV est la suivante :
- le directeur ou son représentant ;
- le directeur des soins ou son représentant ;
- le président de la commission médicale d'établissement (CME) ou son représentant ;
- le médecin de l'information médicale (DIM) ou son représentant ;
- le responsable du service ou de la direction qualité gestion des risques (CQGR) ou son représentant ;
- le coordonnateur de la gestion des risques associés aux soins ;
- le référent en identitovigilance ou son représentant ;
- le directeur ou le responsable des systèmes d'information (RSI) ou son représentant ;
- le responsable de la sécurité des systèmes d'information
- le délégué à la protection des données (DPD) de la structure ;
- le responsable du bureau des entrées ;
- le correspondant en identitovigilance des services médico-techniques :
    - laboratoire de biologie médicale,
    - laboratoire d'anatomie et de cytologie pathologique,
    - pharmacie à usage intérieur,
    - bloc opératoire…
- le correspondant en identitovigilance du service des urgences ;
- un correspondant en identitovigilance d'un service clinique ;
- un représentant des structures partenaires (sous-traitants et prestataires) ;
- les référents logiciel ;
- un représentant des usagers.

La composition du COSTRATIV est actualisée annuellement et est disponible dans la gestion documentaire (*indiquer ici le nom de la GED*).

L''établissement rédige un règlement intérieur pour préciser les modalités de fonctionnement du COSTRATIV.

b) Missions

Les missions du COSTRATIV sont les suivantes :

- définir la politique d'Identitovigilance de l'établissement et décliner son plan d'action annuel *en veillant à la cohérence des documents de l'établissement avec les documents du groupement ou du GHT ;*
- arrêter l'organisation à mettre en œuvre (instances, missions confiées) ;
- définir les moyens humains, techniques et financiers à attribuer pour le fonctionnement optimal de cette organisation ;
- définir la politique de formation en identitovigilance conduite dans l'établissement *en cohérence avec la politique définie par l'instance du groupement ou GHT*, et s'assurer de sa mise en œuvre ;
- mettre en place un système d'évaluation et de suivi qualité (indicateurs, audits, suivi et analyse des évènements indésirables liés à l'identification de l'usager…) *en cohérence avec celui défini dans le groupement* ;
- s'assurer de la bonne gestion des documents qualité relatifs à l'identification de l'usager au sein de l'établissement *et de leur cohérence avec les documents qualité communs au groupement* ;
- participer à la gestion des risques en identitovigilance :
    - gestion des risques *a priori* : cartographie des risques de l'établissement,

  - gestion des risques *a posteriori* : suivi des évènements indésirables et actions correctives, préventives ou d'atténuation à mettre en œuvre ;
- s'assurer de la bonne application des procédures concernant l'identification et les bonnes pratiques professionnelles, conformément à la réglementation *et aux recommandations du groupement ou du GHT* ;
- collecter, analyser et résoudre les problématiques locales liées aux actions d'identification ;
- alerter la direction de l'établissement sur les éventuels problèmes ou dysfonctionnements dans la mise en œuvre de la politique et/ou de la charte d'identitovigilance ;
- *alerter l'instance décisionnaire du groupement ou du GHT sur des problèmes survenant aux interfaces de deux établissements partie ou associés au groupement*
- signaler des événements indésirables graves en rapport avec l'identification des usagers sur le portail de signalement des évènements sanitaires indésirables ;
- formaliser 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 ;
- *communiquer annuellement le bilan d'activité à l'instance décisionnaire du groupement ou du GHT*.

c) Fréquence de réunions

Le COSTRATIV se réunit au moins deux fois par an.

2. La cellule opérationnelle d'identitovigilance (COIV)

Objet du chapitre : préciser les missions et la composition de la structure chargée au quotidien de la gestion des problématiques d'identitovigilance.

La COIV est une instance opérationnelle d'identitovigilance du *CH mettre ici le nom de la structure*. Elle dispose de *mettre ici le nombre d'ETP affectés à la COIV* ETP. Le nombre d'ETP dédiés est en adéquation avec les besoins de l'établissement. Les personnels affectés dans cette cellule sont aguerris en identitovigilance. *La structure peut renvoyer aux attestations de formation des personnels et à leur qualification.*

Elle a pour missions de :
- 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 sur la base du plan de formation continue validé par le COSTRATIV en accord avec le service formation ;
- participer à la formation continue des soignants en charge de l'identification secondaire ;
- rédiger et actualiser les documents qualité relatifs à l'identification primaire ou secondaire de l'usager ;
- maintenir la qualité de la base patient locale en résolvant les problèmes liés à l'identification primaire (fusion de doublons, défusion de collision…) ;
- contrôler la qualité des bases de données utilisées par la structure ;
- *contribuer au rapprochement d'identité entre établissement en statuant sur les identités proposées au rapprochement inter établissement (si l'établissement participe à un rapprochement d'identités)* ;
- recueillir et analyser les évènements indésirables en lien avec l'identitovigilance en lien avec le service qualité gestion des risques ;
- recueillir et analyser les indicateurs qualité.

Les actions menées par la COIV alimentent le plan d'action et le bilan d'activité de la thématique identitovigilance.

Le fonctionnement de la COIV est précisé dans un règlement intérieur.

3. Le référent en identitovigilance

Objet du chapitre : préciser les missions du référent en identitovigilance de la structure.

Le référent en identitovigilance doit être nommé (note de désignation de la direction) et disposer d'une lettre de mission ou d'une fiche de poste (vous pouvez vous appuyer sur la lettre de mission proposée par le GRIVES).

Le référent local en identitovigilance est désigné par le directeur de l'établissement et le président de la CME (cf. note de désignation présente dans la gestion documentaire *mettre ici le nom de la GED*).

Point d'attention : il est fortement préconisé que le référent en identitovigilance de la structure soit identifié dans le répertoire opérationnel des ressources (ROR). Il doit disposer de la compétence particulière « identitovigilance » sur sa fiche professionnelle.

L'établissement complète les missions du référent en identitovigilance si nécessaire.

- Le référent en identitovigilance de l'établissement est membre de droit du comité stratégique d'identitovigilance de l'établissement (COSTRATIV).
- *Il participe au comité stratégique d'identitovigilance territorial.*
- Il assure la supervision technique des activités de la cellule opérationnelle d'identitovigilance (COIV).
- Il organise l'identitovigilance au sein de l'établissement conformément aux exigences règlementaires (RNIV) et aux bonnes pratiques d'identitovigilance.
- Il est l'interlocuteur privilégié de la direction de l'établissement, de la CME, de l'ensemble du personnel pour toutes les problématiques liées à l'identification de l'usager (identification primaire et secondaire).
- Il participe à l'élaboration de la politique d'identification des usagers en lien avec la direction, la CME et le COSTRATIV, le coordonnateur de la gestion des risques associés aux soins, le directeur ou le responsable qualité de l'établissement.
- Il organise et/ou anime les réunions du COSTRATIV.
- Il assure la veille réglementaire et technique en matière d'identitovigilance.
- Il s'assure de l'adéquation des pratiques avec les exigences de l'identitovigilance.
- Il participe à l'élaboration des plans de crise en particulier l'organisation de l'identification des victimes.
- Il contribue aux travaux de convergence des systèmes d'information du GHT ou du groupement mettre ici le nom du groupement auquel appartient mettre ici le nom de la structure en matière d'identitovigilance ;
- Il participe au choix des outils et donne un avis d'expert sur leur conformité aux exigences des référentiels (RNIV, guide d'implémentation de l'INS…) et leur adéquation aux besoins de la structure en termes d'identification de l'usager.
- Il supervise le suivi (rédaction, révision) des documents qualité (procédures, modes opératoires, fiches réflexes…) nécessaires à l'organisation et au suivi de l'identitovigilance au sein de l'établissement / *du groupement ou du GHT*.
- Il participe à la gestion des risques *a priori* et *a posteriori*.
- Il élabore ou s'assure de l'élaboration du plan d'actions annuel et de son suivi et établit le rapport annuel d'activités.
- Il définit, en lien avec le COSTRATIV, le service qualité, le coordonnateur de la gestion des risques associés aux soins, la cellule opérationnelle d'identitovigilance, le planning annuel des évaluations, s'assure de leur réalisation et participe à l'analyse des résultats et à la définition des plans d'actions et de leur mise en place.
- Il s'assure de la formation et de la sensibilisation du personnel en matière d'identitovigilance, en particulier, des règles de vérification de l'identité des usagers en lien avec le service formation continue de l'établissement.
- Il supervise le maintien de la qualité du référentiel identité de l'établissement / *du groupement ou du GHT* en particulier de la détection et du traitement des doublons potentiels, de la gestion des collisions, des anomalies liées à l'INS, *du traitement des rapprochements d'identités*.
- Il est responsable de la diffusion et de la gestion des alertes d'identitovigilance internes et externes dans son établissement.
- Il assure le suivi des indicateurs d'identitovigilance définis au niveau de l'établissement / *du groupement ou du GHT* et leur analyse.
- Il assure le suivi des déclarations des évènements indésirables relatifs à l'identification de l'usager et participe à leur analyse et à la mise en place d'actions d'amélioration.
- Il assure, dans le cadre de la procédure de certification, l'évaluation du critère 2.3-01 « les équipes respectent les bonnes pratiques d'identification du patient à toutes les étapes de sa prise en charge ».

- Il assure la communication interne et externe autours de l'identitovigilance :
  - vers la commission des soins infirmiers, de rééducation et médico-techniques (CSIRMT), Commission médicale d'établissement…),
  - vers des instances régionales,
  - vers les personnels de l'établissement,
  - *vers les instances de groupement ou de GHT*.
- Il participe au réseau régional du GRIVES.

Il rend compte à la direction de l'établissement et à la CME *et au comité stratégique de groupement ou de GHT* de l'ensemble de ses activités, de toute difficulté rencontrée et des problématiques relatives à l'identitovigilance survenant dans son établissement.

4. Correspondants en identitovigilance

Objet du chapitre : préciser les missions des professionnels correspondants de la structure opérationnelle identifiés dans les services et les structures partenaires (si applicable).
La désignation de correspondants en identitovigilance n'est pas rendue obligatoire par le RNIV mais elle est fortement conseillée pour assurer une bonne diffusion de l'information et une bonne remontée des incidents.

a) Correspondants en identitovigilance internes

Chaque service clinique et médicotechnique dispose d'un correspondant en identitovigilance.

Décrire ici les critères de choix des correspondants en identitovigilance :

Choix 1 possible : désigner systématiquement un personnel d'encadrement, par exemple :
Proposition de rédaction :
Les correspondants en identitovigilance des unités de soins et médico-techniques sont :
- les secrétaires référents de pôles ou d'unité de soins en ce qui concerne l'identification primaire du patient ;
- les cadres de santé en ce qui concerne l'identification secondaire du patient ;
- le chef de service clinique ou médico-technique en ce qui concerne l'identification secondaire du patient.

Choix 2 possible : désigner un personnel selon son appétence pour la thématique dans ce cas il est indispensable de prévoir une note de désignation nominative réactualisée annuellement.
Proposition de rédaction
Les correspondants en identitovigilance des unités de soins et des services médico-techniques sont identifiés pour leur appétence et leur compétence en identitovigilance. Une note de désignation nominative réactualisée annuellement est disponible dans la gestion documentaire.

Description des missions des correspondants en identitovigilance :
Le correspondant en identitovigilance est l'interlocuteur privilégié de la COIV, du référent en identitovigilance.

- Il participe aux réunions de l'instance décisionnaire lorsqu'il y est invité.
- Il fait le lien et transmet les informations nécessaires dans l'unité de soins (durant les relèves, staffs et autres réunions de l'unité de soins).
- Il participe au déroulement des audits et des enquêtes qui ont lieu dans l'unité de soins.
- Selon les besoins, il participe avec les membres de la COIV à l'organisation des différents types de formation du personnel de son unité de soins.
- Il diffuse les informations descendantes et informe le référent en identitovigilance et la COIV des dysfonctionnements ou problématiques en relation avec l'identification de l'usager, rencontrés dans son unité de soin.

- Il s'engage promouvoir la déclaration des EIG relatifs à l'identitovigilance dans le respect des règles institutionnelles de déclaration et la déclaration de tous les EI fréquents pour identifier des évènements porteurs de risques.

La liste des correspondants en identitovigilance est disponible dans la gestion documentaire et est à disposition des personnels.

b) Correspondants en identitovigilance externes

Objet du chapitre : préciser le rôle des correspondants externes en identitovigilance.

Les structures partenaires, sous-traitants et clients (cabinet d'imagerie médicale, laboratoire de biologie, laboratoire d'anatomie et de cytologie pathologiques…) sont invités à identifier des correspondants en identitovigilance et à transmettre leurs coordonnées à la COIV de l'établissement. La connaissance du correspondant en identitovigilance de facilite la mise en commun des règles d'identitovigilance, le signalement et le traitement des erreurs dans le cadre des données de santé échangées.
Ces correspondants sont invités à participer aux réunions et actions de la COIV pour les sujets qui les concernent et peuvent être conviés aux réunions du COSTRATIV.
La COIV et les structures partenaires disposent chacune de la liste de l'ensemble des référents et correspondants en identitovigilance. Elle est mise à jour en tant que besoin dans la GED.

c) Référents logiciels

Objet du chapitre : préciser le rôle des référents logiciels. Les référents logiciels doivent être identifiés, désignés et disposer d'une lettre de mission. Vous pouvez vous appuyer sur la lettre de mission proposée par le GRIVES.

Le système d'information de la structure comporte plusieurs applications informatiques dédiées participant au processus de soin.
Pour chaque application, un référent logiciel métier est désigné. Dans le domaine de l'identitovigilance, ce référent est le correspondant de la COIV. Son rôle est notamment d'assurer la cohérence des données avec le référentiel d'identités de l'établissement, notamment lors des opérations liées au traitement des doublons ou erreurs d'identités, de participer en lien avec le service informatique et la COIV aux tests d'interfaces d'identités. Les référents logiciels disposent d'une lettre de mission. La liste de ces référents est actualisée annuellement, elle est disponible, ainsi que leur lettre de mission, dans la gestion documentaire.

DEFINITIONS ET TERMINOLOGIE

Objet du chapitre : préciser les définitions des termes employés dans les documents d'identitovigilance de la structure.

L'objet de ce chapitre est de rappeler la signification des termes techniques utilisés dans l'établissement 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 *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.

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.

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 (cf. 5).

Identifiant numérique : séquence de caractères qu'un ou plusieurs domaines d'identification (cf. 3) utilisent pour représenter une personne et lui associer des informations dans le cadre de sa prise en charge.

Identité nationale de santé (INS) : ensemble de traits constituant l'identité sanitaire officielle d'un usager de la santé, tels qu'ils sont enregistrés dans des bases nationales. L'identité nationale de santé est composée de 5 traits stricts de références (nom de naissance, prénom(s), sexe, date de naissance, code du lieu de naissance (commune ou pays pour un usager nés à l'étranger), d'un matricule INS qui a pour valeur le NIR (numéro d'identification au répertoire des personnes physiques) ou le NIA (numéro d'identification d'attente) de l'individu.

3. Domaine d'identification

Le domaine d'identification (DI) regroupe au sein d'une organisation de santé toutes les applications qui utilisent le même identifiant pour désigner un patient.
Exemple 1 : un cabinet médical disposant d'un mode unique d'identification de ses usagers est considéré comme un domaine d'identification.
Exemple 2 : un établissement de santé dont tous les logiciels utilisent le même identifiant est un domaine d'identification.

4. Domaine de rapprochement

Le domaine de rapprochement (DR) rassemble au moins deux domaines d'identification qui échangent ou partagent des informations entre eux. On distingue les domaines de rapprochements intra établissement et extra établissement.
Exemple 3 : un établissement de santé disposant d'un Identifiant Permanent du Patient (IPP) et dont une partie des logiciels utilise un identifiant et une autre partie des logiciels un autre identifiant est un domaine de rapprochement. En effet, dans cet exemple, il existe deux groupes de logiciels et chaque groupe utilise un identifiant qui lui est propre. Chaque groupe constitue donc un domaine d'identification différent. L'établissement dispose également d'un IPP qui lui permet d'échanger des informations entre les deux domaines d'identification. Ce domaine de rapprochement est un domaine de rapprochement intra établissement.
Exemple 4 : si des établissements de santé alimentent un serveur régional d'identité, alors ce serveur constitue un domaine de rapprochement.

5. Traits d'identification

Les traits d'identification sont les informations définies dans un système d'information comme constituants de l'identité numérique d'un usager. Exemple de traits : nom de naissance, nom utilisé, prénom de naissance, prénom utilisé, date de naissance, sexe. On distingue :

- 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 stricts sont stables dans le temps pour la très grande majorité des usagers.
- 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.

6. 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.

7. Doublons, fusions, collisions

Le **doublon d'identités numériques** correspond à l'identification d'une même personne sous au moins deux identifiants numériques 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 qualifier ce couple de doublon avéré s'il s'agit réellement d'un doublon 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'IPP conservé est alors appelé IPP maitre et l'IPP fusionné, 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 2 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). Ces situations de non-qualité sont particulièrement difficiles à corriger.

LA GESTION DE L'IDENTITE

Objet du chapitre : décrire la gestion de l'identité au sein de la structure, en termes de traits utilisés, de système d'information, de pratiques.
Exemple de rédaction :

1. Le domaine d'identification

Objet du chapitre : décrire le domaine d'identification.

Le *CH indiquer ici le nom de votre structure* dispose d'un référentiel unique d'identité pour toutes les applications participant au processus de soins, conformément aux exigences du prérequis P1.1 du programme HOP EN. L'ensemble des applications est alimenté en identité par le référentiel unique d'identité *mettre ici le nom du référentiel*. La cartographie applicative du *indiquer ici le nom de votre structure (renvoyer à la cartographie applicative par un lien hypertexte par exemple)* 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. *Si vous disposez d'autres types d'interfaces (HPIRM santé par exemple) ou d'interfaces propriétaires non conformes aux standards normés, le préciser. Dans la gestion des risques il sera nécessaire de prévoir un chapitre supplémentaire décrivant comment sont maitrisées ces interfaces propriétaires.*

Si la structure ne dispose pas d'un référentiel unique d'identité, il est nécessaire de décrire ici les outils non alimentés par le référentiel et dans le chapitre gestion des risques, il faudra décrire les process mis en œuvre pour sécuriser l'identification de l'usager.

Le fait de disposer d'un référentiel unique identité est une exigence du RNIV et un prépequis du programme HOP EN (P1.1). La présence d'un référentiel unique d'identité permet de sécuriser l'utilisation des identités numériques.

2. Les identifiants utilisés dans l'établissement

Objet du chapitre : décrire les identifiants utilisés dans l'établissement.
Point d'attention, le matricule INS pouvant varier dans certains cas, il n'est pas considéré ici comme un identifiant mais comme un trait strict de d'identité

Les identifiants numériques utilisés dans l'établissements sont :

- l'identifiant permanent patient (IPP), identifiant unique du dossier de l'usager et associé à son identité ;
- l'identifiant d'épisode patient (IEP) ou numéro de séjour, qui identifie le séjour ou la venue et est relié à l'IPP du dossier. Un nouvel IEP est créé à chaque venue de l'usager.

3. Les lieux de création de l'identité

Objet du chapitre : décrire les lieux de création de l'identité dans l'établissement. L'établissement supprime les items non pertinents et adapte le tableau en fonction de ses pratiques.
Il est rappelé que la création des identités par les soignants doit être limitée à des cas très particulier.

Les lieux de création d'identité ainsi que les fonctions des personnels dans l'établissements sont décrits dans le tableau suivant.

Service/lieu	Période	Fonction des personnels	Commentaire
Bureau des entrées	Heures ouvrables	Admissionnistes	
Service des urgences	Heures ouvrables	Secrétaire médicale/admissionnistes	
Service des urgences	Permanence des soins	Personnel soignant *(préciser la fonction)*	
Maternité	Heures ouvrables et permanence des soins	Sages-femmes	Création de l'identité des nouveaux nés Création de l'identité des parturientes si non connues

4. Les traits d'identification

Objet du chapitre : préciser les traits d'identification et les règles de saisie de l'identité retenues dans la structure.

Le *CH indiquer ici le nom de la structure* respecte les exigences du RNIV en matière de traits d'identification. Les traits d'identification utilisés sont les suivants :

a) 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[1]).

b) Traits complémentaires

La structure adaptera les traits complémentaires proposés en fonction de ses pratiques.
*La saisie des traits complémentaires identifiés par une * est rendue obligatoire par le RNIV.*
*La saisie des traits complémentaires identifiés par une * est très fortement préconisée en région PACA.*

- *Nom utilisé** (saisie obligatoire si différent du nom de naissance);
- *Prénom utilisé** (saisie obligatoire si différent du premier prénom de naissance);
- *Code postal* de la commune de naissance (pour les usagers nés en France exclusivement) *;
- *Commune de naissance** ;
- *Adresse de résidence* de l'usager* ;
- Numéros de téléphone (portable et fixe)* ;
- Adresse(s) courriel de contact* ;
- Nom des personnes en relation (parents, enfant, conjoint, personne de confiance, personne à prévenir…) ;
- 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* *(attention, il ne faut pas saisir le numéro de la pièce)*.

c) Politique de la structure concernant la saisie des noms et prénoms utilisés

Objet du chapitre : ce chapitre vise à décrire la politique adoptée par l'établissement.
Pour mémoire : le RNIV rend possible la saisie dans les champs nom et prénom utilisés d'éléments ne figurant pas sur la pièce d'identité présentée par l'usager. La structure doit choisir :
- *soit de recopier à l'identique une pièce d'identité ;*
- *soit de permettre la saisie d'un nom ou d'un prénom non présent sur une pièce d'identité ;*
- *soit de permettre de ne pas saisir un nom ou un prénom présent sur une pièce d'identité.*

Trois rédactions sont proposées selon les choix qui peuvent être faits par l'établissement. L'établissement supprime les éléments proposés non pertinents.

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

Le *CH mettre ici le nom de la structure* : a fait le choix de :

Choix 1 possible : recopier à l'identique les éléments d'identité présents sur la pièce d'identité présentée par l'usager, *ie*
- 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 explicitement 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).

Choix 2 possible : ne pas saisir un nom utilisé y compris s'il est présent sur une pièce d'identité si l'usager ne le souhaite pas. L'établissement a mis en place une organisation permettant lors des éventuels contrôles à distance de l'identité de s'assurer qu'il ne s'agit pas d'une erreur du professionnel de l'accueil. *(L'établissement décrit ici l'organisation adoptée : document rempli par l'usager et scanné dans le dossier par exemple).*

Choix 3 possible : saisir un nom utilisé ou un prénom utilisé non présents sur la pièce d'identité, à la demande de l'usager. L'établissement a mis en place une organisation permettant lors des éventuels contrôles à distance de l'identité de s'assurer qu'il ne s'agit pas d'une erreur du professionnel de l'accueil. *(L'établissement décrit ici l'organisation adoptée : document rempli par l'usager et scanné dans le dossier par exemple).*

Si la structure pratique le double nommage, (saisie systématique d'un nom utilisé y compris s'il est identique au nom de naissance et/ou saisie systématique d'un prénom utilisé y compris s'il est identique au premier prénom de naissance) il est nécessaire de l'indiquer ici. La pratique du double nommage n'est pas conseillée, cependant les structures peuvent être contraintes par les fonctionnalités de leur système d'information et en particulier de leurs outils métier.

Choix 1 possible : La structure a fait le choix de pratiquer le double nommage en ce qui concerne les champs (*la structure adapte la proposition et supprime par exemple le double nommage pour le champ prénom utilisé, si elle ne le pratique pas)* :
- nom utilisé : ce champ sera systématiquement rempli y compris si l'usager utilise uniquement son nom de naissance dans la vie courante (recopie du nom de naissance dans le champ nom utilisé) ;
- prénom utilisé : ce champ sera systématiquement rempli y compris si l'usager utilise uniquement son premier prénom de naissance dans la vie courante (recopie du premier prénom de naissance dans le champ prénom utilisé).

Choix 2 possible : la structure ne pratique pas le double nommage :
- le champ nom utilisé n'est renseigné que si l'usager utilise un nom différent de son nom de naissance ;
- le champ prénom utilisé n'est renseigné que si l'usager utilise un prénom différent de son premier prénom de naissance.

5. Recherche, création, qualification d'une identité

a) 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. *Cette pratique permet d'améliorer le dépistage des erreurs (erreur de sélection d'une pièce d'identité par l'usager s'ils en possèdent plusieurs – celles des enfants mineurs par exemple – et des usurpations d'identité.*

b) Recherche d'une identité

Objet du chapitre : Décrire les principes de recherche d'une identité dans l'établissement
L'établissement adapte la rédaction proposée en fonction de ses pratiques. La recherche par date de naissance est recommandée par le RNIV.

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, l'établissement a fait le choix de compléter la date de naissance par les x premiers caractères du nom *et/ou* par les y premiers caractères du prénom.

La structure adapte le paragraphe ci-dessous selon les fonctionnalités proposées par le logiciel.
Le système d'information permet la recherche d'une chaine 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.

Il est possible de rajouter la phrase suivante si historiquement la structure a enregistré des identités par lecture de la carte vitale par exemple. Compte tenu des particularités du référentiel identité et de l'historique de la gestion des identités dans la structure, si l'usager n'est pas retrouvé en utilisant la recherche par date de naissance, une seconde recherche sera réalisée sans utiliser le critère date de naissance.

c) Création d'une identité

Objet du chapitre : Décrire les principes création d'une identité. Il est proposé ici de distinguer la création d'une identité en heures ouvrables par des professionnels de l'accueil et la création d'une identité réalisée en heure de permanence des soins par des soignants.

Conformément au RNIV, les traits obligatoires pour créer une identité sont :
- le nom de naissance ;
- le nom utilisé *(à ne conserver que si la structure pratique du double nommage sur le champ nom utilisé)*
- le premier prénom de naissance ;
- le prénom utilisé (*à ne conserver que si la structure pratique le double nommage sur le champ prénom utilisé)*
- le sexe ;
- la date de naissance ;
- le code INSEE du lieu de naissance : le système d'information de la structure propose automatiquement un code de lieu de naissance si la ville et/ou le code postal du lieu de naissance sont saisis.

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]

et par les traits complémentaires suivants *(l'établissement liste ici les traits complémentaires qui doivent être obligatoirement saisis : par exemple)* :
- ville et code postal de naissance
- adresse postale
- adresse courriel
- numéro de téléphone ;
- médecin traitant
- personne à prévenir
- personne de confiance…

Le processus détaillé de création d'une identité est décrit dans une procédure. Seuls les éléments structurants sont repris ici.

i. Les règles de saisies de l'identité

Objet du chapitre : décrire les règles de saisie d'une 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.

[2] Usagers nés ou travaillant en France

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

Objet du chapitre : décrire la politique de la structure concernant l'appel au téléservice et décrire les modalités utilisées pour l'appel.

Choix concernant le statut des identités :
Choix 1 possible : l'établissement a fait le choix de n'appeler le téléservice que si l'identité de l'usager est au statut identité validée.

Choix 2 possible : l'établissement a fait le choix d'appeler le téléservice pour les identités au statut identité provisoire. L'établissement a mis en place une organisation de validation des identités en back office (cf. infra).

Choix concernant les modalités d'appel :
Choix 1 possible : la structure privilégie l'appel au téléservice par lecture de la carte vitale.

Choix 2 possible : la structure privilégie l'appel au téléservice par saisie des traits.

Cas particulier des établissements disposant d'une maternité : il est nécessaire de préciser ici la politique concernant la récupération de l'INS pour les nouveau-nés.

Choix 1 possible : L'établissement fait le choix de récupérer l'INS en backoffice quelques jours après la naissance du nouveau-né.

Choix 2 possible : L'établissement qualifiera l'identité du nouveau-né lors d'une venue ultérieure.

iii. Création des identités en heures ouvrables par les professionnels de l'accueil

Plusieurs processus de création d'identité sont proposés. L'établissement ne conserve que les éléments adaptés à ses pratiques.

Choix 1 possible : Si l'usager est éligible à l'INS, l'établissement a fait le choix de créer une identité à partir des traits récupérés lors de l'appel à l'opération de récupération du téléservice INSi.
Cette identité est ensuite complétée par les traits cités infra.

Choix 2 possible : L'établissement fait le choix de créer systématiquement une identité locale avant de réaliser l'appel au téléservice INSi pour les usagers éligibles.

iv. Création des identités en heures de permanence des soins par les soignants

Proposition d'organisation :
Les soignants créent une identité locale. La récupération de l'INS est réalisée par la cellule opérationnelle d'identitovigilance en backoffice après réalisation d'un contrôle de cohérence entre l'identité numérique locale et les traits présents sur une pièce d'identité de haut niveau de confiance.

d) Les attributs de l'identité

Objet du chapitre : décrire l'utilisation des attributs de l'identité dans l'établissement. L'établissement modifie la rédaction proposée selon ses pratiques. A noter que l'utilisation des attributs identité douteuse ou identité fictive est fortement recommandée par le GRIVES.

L'établissement utilise les attributs :
- 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 incapables de décliner leur identité, anonymat par exemple) ;
- identité homonyme pour attirer l'attention des professionnels sur la présence d'identités approchantes dans le référentiel identité.

e) Le processus de validation des identités et de qualification de l'INS

Objet du chapitre : décrire l'organisation de l'établissement pour la validation des identités et la qualification des INS. Il est fortement recommandé qu'un process de validation en FrontOffice s'accompagne d'une demande de vérification des traits saisis par l'usager (sur une planche d'étiquette, sur un document de circulation, une fiche administrative…).

Choix 1 possible : 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.
Avant cette opération de validation, il est demandé à l'usager ou à son accompagnant de contrôler l'exactitude des informations saisies sur un support (*préciser ici le support utilisé)*.

Choix 2 possible : La validation des identités est réalisée en back office par la cellule opérationnelle d'identitovigilance après réalisation d'un contrôle de cohérence entre l'identité numérique et l'identité présente sur la pièce d'identité. La pièce d'identité numérisée est disponible dans le référentiel identité.

f) 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 ;
- passeport ;
- titre de séjour permanent ;
- pour les mineurs, livret de famille ou extrait d'acte de naissance accompagné de la pièce d'identité du responsable légal ;
- dispositif d'identification électronique de niveau substantiel.

L'établissement dispose d'un outil de numérisation des pièces d'identité. Ces pièces sont conservées dans les conditions précisées dans la FIP06 Gestion des copies de pièces d'identité dans le système d'information proposée par le réseau 3RIV (*Cette mention est à supprimer si la structure ne dispose pas d'outil de numérisation).*

.

g) Les identités particulières

Objet du chapitre : décrire de façon macroscopique les identités particulières pouvant être utilisées par l'établissement.

L'établissement peut utiliser des identités fictives dans les situations suivantes *(l'établissement supprime les situations qui ne sont pas pertinentes au regard de son activité)* :
- usager inconscient incapable de décliner son identité ;
- situations légales d'anonymats (accouchement dans le secret, centre de désintoxication) ;

- à la demande d'un usager qui souhaite être pris en charge sans divulgation de son identité (VIP par exemple, personnel de l'établissement) ;
- pour réaliser des tests informatiques (patients tests) ;
- lors de l'accueil d'afflux massif de victimes lors de situations sanitaires exceptionnelles.

La création de ces identités fictives fait l'objet d'une procédure, d'une formation particulière des personnels.

La structure peut donner ici les grands principes de création des identités fictives ou renvoyer à la procédure had hoc. Le fait de donner les grands principes dans la charte, ne dispense pas de disposer d'une procédure spécifique.

La procédure identité fictive doit prévoir en particulier :
- *Les règles de nommage : il est recommandé d'utiliser une date de naissance cohérente avec l'âge apparent de l'usager, de compléter la chaine de caractère choisie pour le nom par un numéro incrémental (date du jour par exemple). Le réseau 3RIV propose plusieurs fiches pratiques et un memento sur lesquels l'établissement peut s'appuyer pour définir les règles de nommage.*
- *La procédure de rectification de ces identités (hors cas légaux d'anonymat) et d'information des partenaires.*

Si l'établissement transmet des identités à un autre référentiel (exemple référentiel régional d'identité), il s'assurera d'utiliser une procédure permettant de mettre en place des filtres sur son EAI afin de ne pas transmettre ces identités fictives.

Les patients tests doivent être parfaitement identifiables, il est proposé d'utiliser les règles de saisie décrites ci-dessous :
- *Champ Nom : TEST+Nom complet de l'établissement ;*
- *Champ Nom de naissance : à discrétion du testeur pour différencier le patient test ;*
- *Champ Prénom : à discrétion du testeur pour différencier le patient test ;*
- *Champ Sexe : M ou F selon les besoins du test ;*
- *Champ Date de naissance : à choisir selon les besoins du test.*

L'identité des usagers détenus ou gardés à vue fait également l'objet d'une attention particulière et d'une procédure formalisée (utilisation de l'attribut identité douteuse si nécessaire, identités restant au statut identité provisoire).

6. Identification primaire sans présence physique de l'usager.

Objet du chapitre : décrire les modalités d'identification primaire mises en œuvre par l'établissement si une identité doit être enregistrée dans le référentiel d'identité en l'absence de l'usager.

a) Téléconsultation

L'établissement décrit ici le processus de sécurisation de l'identité si l'usager bénéficiant de la téléconsultation n'est pas connu dans le référentiel identité (des propositions sont présentes dans l'annexe V du RNIV1)

b) Identités transmises à un sous-traitant, télé-expertise…

Conformément au RNIV, l'établissement a inclus une clause de confiance dans les contrats qui le lient à ses sous-traitants ou partenaires.

7. Le maintien de la qualité du référentiel identité.

Objet du chapitre : décrire l'organisation du signalement des anomalies et de leur traitement.

Le maintien de la qualité du référentiel identité est sous la responsabilité de la cellule opérationnelle d'identitovigilance.
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 et le traitement des anomalies sont formalisés dans une procédure à disposition des personnels.

Il est conseillé de disposer de deux procédures, une de signalement à destination des personnels de l'établissement, l'autre de traitement à destination des personnels de la COIV.
La procédure de signalement doit comporter :

- *les anomalies qui doivent être signalées ;*
- *le moyen de signalement (mail, outil dédié type logiciel d'identitovigilance, portail intranet de l'établissement, fax…) ;*
- *les éléments indispensables au signalement (qui peuvent être présents dans un formulaire à remplir) ;*
- *les suites données au signalement ;*
- *l'information rétroactive des personnels.*

La procédure de traitement des anomalies doit comporter :

- *le type d'anomalies traitées (collision, doublon, erreur sur une identité, erreur sur une INS…) ;*
- *les acteurs en charge du traitement ;*
- *les vérifications réalisées au cours du traitement ;*
- *la politique de fusion en termes d'identité numérique à conserver (IPP le plus ancien,, dossier le plus riche, identité de plus haut niveau de confiance…) ;*
- *la traçabilité des actions*
- *le temps du traitement (la fusion est-elle réalisée au cours de l'hospitalisation ou après la sortie ?, aucune modification n'est réalisée au cours d'un acte à risque (transfusion, bloc opératoire)…)*
- *l'information des personnels et services de l'établissement (a minima banque du sang, laboratoires, services d'hospitalisation) ;*
- *l'information des partenaires hors du domaine d'identification (sous-traitants par exemple), en particulier si les modifications ne peuvent être propagées par des flux d'interopérabilité ;*
- *la répercussion des fusions et/ou des modifications d'identités dans les outils incomplètement ou non interfacés ;*
- *la prise en compte du traitement des collisions dans les outils métiers (RIS, PACS, laboratoire, DPI…) en précisant en particulier l'identification de l'acteur en charge (correspondant d'identitovigilance du service par exemple) ;*
- *la réimpression éventuellement nécessaire de documents (bracelet, étiquettes…)*

L'établissement peut décrire ici brièvement le circuit par exemple :

L'établissement dispose d'un outil informatisé de signalement des anomalies. Les professionnels utilisent un formulaire dédié. Les anomalies traitées alimentent le tableau de bord de pilotage….

8. Droits d'identification

Objet du chapitre : décrire les droits liés à l'utilisation des identités dans l'établissement.

Un exemple de présentation sous forme de tableau vous est proposé ci-dessous, renseigné avec les organisations les plus courantes. L'établissement doit modifier le tableau proposé en fonction de son organisation.
Pour mémoire, il est fortement conseillé de limiter les droits de modifications d'identité (bureau des entrées et cellule opérationnelle d'identitovigilance). Il est préconisé de ne pas donner les droits d'appel au téléservice INSi aux soignants (qui ne sont pas des professionnels de l'accueil).

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

Service/lieu	Application utilisée	Recherche et consultation d'une identité	Création identité locale	Appel au téléservice	Modification d'identité	Validation d'identité	Fusion Défusion de collision	Déqualification, suppression d'une INS
Bureau des entrées	Référentiel identité	X	X	X	X	X		
Service des urgences	Référentiel unique d'identité ou outil métier relié au référentiel unique d'identité	X	X					
Secrétariat services cliniques et médico-techniques	*Référentiel unique d'identité ou DPI* relié au référentiel unique d'identité	X	*Dans l'outil métier en mode dégradé (indisponibilité du référentiel identité*		*Uniquement adresse, téléphone, mail, médecin traitants (traits complémentaires hors nom et prénom utilisés*			
Services cliniques et médico-techniques personnel soignant	*DPI* relié au référentiel unique d'identité	X						
Cellule opérationnelle d'identitovigilance	*Référentiel unique d'identité ou. DPI*	X	X	X	X	X	X	X

FIABILISATION DE L'IDENTIFICATION SECONDAIRE

Objet du chapitre : décrire les moyens mis en œuvre par la structure pour fiabiliser l'identification secondaire.

1. Le bracelet d'identification

Si la structure n'utilise pas de bracelet d'identification le chapitre est à supprimer

Le *CH indiquer ici le nom de la structure* propose aux usagers de porter des bracelets d'identification. Le port du bracelet est obligatoire pour les usagers non communicants (non francophone, confus, inconscient, dément…). L'information de l'usager, la pose du bracelet et les éléments de contrôle sont formalisés au sein d'une procédure.

Si tous les services de la structure ne sont pas concernés par la pose d'un bracelet, lister les services concernés.
Dans la mesure du possible, il ne doit pas y avoir transcription manuelle de l'identité de l'usager sur le bracelet (source d'erreur).
Il faudra privilégier les bracelets imprimés sur une imprimante dédiée à partir des données du SIH ou les étiquettes imprimées à partir du SIH et collées sur le bracelet.

Les documents qualité nécessaires doivent être rédigés et comprendre :

- *la fiche d'information de l'usager ou de sa famille ou livret d'accueil ;*
- *les éléments de traçabilité de la décision de l'usager et le support d'enregistrement (dossier papier, dossier de soin informatisé).*

Dans chaque structure de santé, le comité d'éthique et/ou la CDU doivent être consultés concernant l'utilisation d'un bracelet d'identification.
Éléments à préciser dans la procédure « dispositif d'identification » de la structure :

- *usagers ou services concernés par la pose du bracelet ;*
- *service créateur du bracelet ;*
- *informations contenues dans le bracelet ;*
- *positionnement du bracelet : sur quel membre le positionner, qui le positionne, à quel moment ;*
- *modalités d'information de l'usager sur la pose et l'utilisation du bracelet d'identification ;*
- *traçabilité dans le dossier de la décision de l'usager ;*
- *vérification des informations portées sur le bracelet (par qui, quand, comment) ;*
- *conduite à tenir en cas de refus de l'usager de pose de bracelet (les mesures barrières qui peuvent être mises en place pour sécuriser l'identification en l'absence de bracelet).*

2. La photographie d'identification

Si la structure n'utilise pas de photographie de l'usager présente dans le dossier pour l'identifier, ce chapitre est à supprimer.

Le *CH indiquer ici le nom de la structure* utilise comme dispositif d'identification de l'usager une photographie présente dans son dossier. L'information de l'usager, la prise de la photographie, l'intégration dans le dossier patient et les éléments de contrôle sont formalisés au sein d'une procédure.

Les documents qualité nécessaires doivent être rédigés et comprendre :

- *la fiche d'information de l'usager ou de sa famille ou livret d'accueil ;*
- *les éléments de traçabilité de la décision de l'usager et le support d'enregistrement (dossier papier, dossier de soin informatisé).*

Dans chaque structure de santé, le comité d'éthique et/ou la CDU doivent être consultés concernant l'utilisation d'une photographie.
Eléments à préciser dans la procédure « dispositif d'identification » de la structure :

- *usagers ou services concernés;*
- *service en charge de la photographie ;*

- *insertion de la photographie dans le dossier;*
- *modalités d'information de l'usager et du recueil du consentement (droit à l'image) ;*
- *traçabilité dans le dossier de la décision de l'usager et du consentement ;*
- *périodicité de renouvellement de la photographie ;*
- *conduite à tenir en cas de refus de l'usager de prise de photographie.*

L'utilisation d'une photographie d'identification nécessite l'information de l'usager et l'obtention d'un accord écrit de sa part, mentionnant les éléments de droits à l'image. Cet accord est conservé dans le système d'information). L'accord de l'usager doit être renouvelé à chaque épisode d'hospitalisation ou selon une périodicité à déterminer par l'établissement pour les établissements médico-sociaux ou les établissements sanitaires de long séjour. La photographie doit être considérée comme une donnée à caractère personnel (article 4 RGPD) et la finalité doit être précisée. La conservation d'une photographie doit être mentionnée dans le registre de traitement de l'établissement.

3. Autre dispositif d'identification

Si la structure utilise un autre dispositif d'identification comme la biométrie par exemple, il est nécessaire de le décrire ici. La biométrie au même titre que la photographie est une donnée à caractère personnel. Elle doit faire l'objet d'un consentement de l'usager et doit être mentionnée dans le registre de traitement (RGPD).

4. Identification de l'usager lors d'un geste ou acte technique

On entend par geste ou acte technique tous les actes médicaux ou paramédicaux réalisés sur l'usager.

Chaque soignant, chaque professionnel, avant la réalisation d'un acte ou d'un soin, vérifie l'identité de l'usager s'il est communicant, en lui posant des questions ouvertes sur *a minima* :

- son nom de naissance ;
- son premier prénom de naissance ;
- sa date de naissance.

Si l'usager est non communicant, l'identité est vérifiée sur le dispositif d'identification.
La cohérence de l'identité est vérifiée avec les supports disponibles (prescription, étiquettes…)
La vérification de l'identité de l'usager par le professionnel est tracée dans le dossier et dans les check-list en vigueur pour la réalisation des actes à risques. *L'établissement peut décrire ici les modalités de traçabilité ou renvoyer à la procédure.*
Une procédure est disponible dans la gestion documentaire.

5. Identification des documents du dossier patient

Le *CH indiquer ici le nom de la structure dispose* d'une organisation et de moyens lui permettant de garantir que tous les éléments du dossier de l'usager sont identifiés et de limiter les erreurs lors de la numérisation de documents dans le dossier patient informatisé.
Décrire ici les moyens mis en œuvre par exemple :

- *tous les documents paramétrés dans le DPI et destinés à être imprimés sont identifiés sur toutes les pages par le nom de naissance, le nom utilisé s'il est différent du nom de naissance , le (s) prénom(s) de naissance, la date de naissance le sexe et l'IPP en-tête ou en en pied de page. SI l'usager dispose d'une INS, l'identité comprend également le code du lieu de naissance ainsi que le matricule INS suivi de sa nature (NIR ou NIA) ;.*
- *la procédure de numérisation des documents dans le DPI est formalisée et limite le risque d'erreur (double contrôle) ;*
- *les personnels en charge du rangement des examens sont formés y compris les internes et les externes en médecine.*

LA GESTION DOCUMENTAIRE

Objet du chapitre : rappeler les modalités de gestion de l'ensemble de la documentation en lien avec l'identitovigilance.
il est proposé ici de lister l'ensemble des types de documents utilisés en identitovigilance.

L'ensemble de la documentation, procédures, modes opératoires, enregistrements, relative à l'identitovigilance sont disponibles dans l'outil de gestion documentaire *mettre ici le nom de l'outil.*
L'alimentation de la GED est sous la responsabilité du service qualité gestion des risques.

1. Procédures

Objet du chapitre : Lister exhaustivement les procédures d'identitovigilance en vigueur dans la structure.
Une procédure est un document qualité reprenant les principes des actions et les grandes étapes. A ne pas confondre avec un mode opératoire, document plus court, pouvant comporter des copies d'écran qui guide de façon détaillée l'utilisateur dans la réalisation d'une action.
L'établissement supprimera de la liste les procédures non pertinentes au regard de son activité et rajoutera les procédures supplémentaires qu'il jugerait utile.
Il est à noter que :
- *les procédures identifiées par une * sont obligatoires quel que soit le type de structure ;*
- *les procédures identifiées par une * sont obligatoires dans les structures disposant d'un service des urgences*

Les procédures en vigueur dans l'établissement sont les suivantes :

- Identification primaire lors de l'accueil de l'usager (recherche d'une identité, création d'une identité, attribution d'un niveau de confiance)*. *Cette procédure peut être déclinée éventuellement selon les points d'accueil (accueil programmé, accueil en urgences, en particulier si les modalités de récupération de l'INS et de la qualification des identités sont différentes…)* ;
- Identification d'un nouveau-né ou d'un enfant à naître, avec les liens mère-enfant *(obligatoire pour les structures disposant d'une maternité)* ;
- Enregistrement de l'identité des enfants nés sans vie *(obligatoire pour les structures disposant d'une maternité)*
- Enregistrement d'un usager incapable de donner ou justifier son identité* ;
- Identification des usagers placés sous main de justice *(obligatoire pour les structures prenant en charge des détenus)* ;
- Identification des victimes lors de situation sanitaire exceptionnelle (afflux massif) * ;
- Admission d'un usager souhaitant garder l'anonymat* ;
- Gestion des cas réglementaires d'anonymat (accouchement dans le secret, cure de désintoxication, etc.) *(obligatoire pour les structures disposant d'une maternité et/ou d'une activité de prise en charge des toxicomanes)*;
- Utilisation d'un dispositif physique d'identification (bracelet d'identification, photographie) * ;
- Identification secondaire d'un usager avant tout acte de soin* ;
- Gestion des transferts entre établissements et au sein de l'établissement* ;
- Signalement des anomalies liées à l'identité (erreurs d'identité, détection de doublons, collisions, usurpation d'identité, erreur de récupération d'un INS, erreur de vérification d'un INS…)* ;
- Prise en charge des anomalies liées à l'identité (correction d'une identité numérique, traitement des doublons, traitement des collisions) * ;
- Gestion des rapprochements d'identités numériques *obligatoire pour les structures* participant à un rapprochement d'identité entre domaine d'identification);
- Gestion d'une suspicion de substitution frauduleuse d'identité* ;
- Information des partenaires après détection d'une erreur d'identification d'un usager* ;

- Gestion des identités dans les logiciels non ou incomplètement interfacés, appartenant à des domaines d'identification différents ou non *(obligatoire pour les structures si certains des logiciels participant à la prise en charge de l'usager sont incomplètement interfacés ou ne sont pas interfacés)* ;
- Mode de fonctionnement dégradé en cas de panne informatique, notamment en termes de gestion de l'identification primaire et secondaire et de reprise d'activité* ;
- Tests des interfaces d'identités* ;
- Gestion des patients tests* ;
- Procédure de gestion et de contrôle qualité des bases d'identités des professionnels de santé comprenant la procédure de déclaration d'un nouvel agent au sein du SIH et la définition des droits d'accès (cette procédure intégrera la gestion des clôtures de compte)*.

2. Modes opératoires

Objet du chapitre : l'établissement peut détailler ici les modes opératoires disponibles. Si certains services (comme le laboratoire ou l'imagerie) disposent d'une GED spécifique il est intéressant de le préciser ici.
Les modes opératoires sont des documents opérationnels permettant de préciser la façon de réaliser des actions. Le mode opératoire comporte en général des copies d'écran.

3. Enregistrements

Objet du chapitre : préciser les enregistrements importants que l'on peut retrouver dans la gestion documentaire. Un enregistrement est un document faisant état de résultats obtenus ou apportant la preuve de la réalisation d'une activité. Les enregistrements doivent être maitrisés (ISO 9001)

*L'établissement liste ici la liste des enregistrements. Les enregistrements signalés par une * doivent obligatoirement être disponibles.*

Les enregistrements suivants sont disponibles dans la gestion documentaire de l'établissement :
- Documents réglementaires et techniques (fiches du réseau 3RIV, fiches GRIVES…) ;
- comptes rendus de réunion du COSTRATIV*, de la COIV ;
- cartographie applicative et schéma des flux* ;
- supports de formations* ;
- Support de communication et de sensibilisation (affiches, flyers…)* ;
- cartes d'identité des indicateurs* ;
- plan d'action* ;
- bilan d'activité* ;
- cartographie des risques *a priori* (cotés et hiérarchisés) ;
- tableau de bord des indicateurs* ;
- grilles et guides d'audits (*si vous utilisez uniquement les grilles et guides d'audits régionaux, vous pouvez renvoyer à l'espace collaboratif GRIVES de l'Agora Social Club*);
- résultats et analyses d'audit* ;
- comptes rendus des analyses réalisées suites à la survenue d'évènements indésirables (Retours, d'expérience, revue de morbi-mortalité…)*.

PILOTAGE

Objet du chapitre : décrire les outils de pilotage de la thématique, indicateurs suivis dans la structure et le mode de suivi, audit réalisés plan d'audit….

Le *CH mettre ici le nom de la structure* suit des indicateurs relatifs à l'identification primaire et à l'identification secondaire. 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 tenu à jour par la COIV et présenté à chaque réunion du COSTRATIV. Après étude en COSTRATIV, il peut être décidé la mise en place d'actions d'amélioration s'il est observé une dégradation des résultats.

1. Indicateurs d'identification primaire

*Les indicateurs listés dans ce chapitre sont les indicateurs proposés par le GRIVES. Les indicateurs identifiés avec une * sont à suivi obligatoire et devront être rendus au niveau national probablement sur la plateforme OSIS (travail en cours par la DGOS) ; le suivi des indicateurs identifiés avec une * est obligatoire en région PACA.*

Les indicateurs suivis dans la structure sont les suivants (*supprimer de la liste les indicateurs non suivis, rajouter éventuellement des indicateurs suivis qui ne seraient pas listés)* :

- taux d'identités nationales de santé ou INS ;
- 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 d'identités présentant un matricule INS identique et des traits d'identités différents ;
- taux de doublon de flux d'INS ;
- part des doublons d'INS dans les doublons ;
- taux de doublon de flux* ;
- taux de doublons traités moins de 72 heures après avoir été dépistés : taux de fusion précoce ;
- nombre et/ou taux de collision* ;
- nombre et/ou taux d'usurpation d'identité* ;
- rapport fusion sur doublon* ;
- taux d'évènements indésirables 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*.

2. Indicateurs d'identification secondaire

*Les indicateurs listés dans ce chapitre sont les indicateurs proposés par le GRIVES. Le suivi des indicateurs identifiés avec une * est fortement recommandé.*

Les indicateurs suivis dans la structure sont les suivants (*supprimer de la liste les indicateurs non suivis, rajouter éventuellement des indicateurs suivis qui ne seraient pas listés)* :

- taux d'évènements porteurs de risques ayant pour origine une erreur d'identification secondaire des usagers* ;
- taux d'évènements indésirables ayant pour origine une erreur d'identification secondaire des usagers* ;
- suivi des non conformités de biologie médicale* ;
- taux de conformité de l'identification des documents du dossier patient ;
- taux de documents référencés avec l'INS*.

3. Formation du personnel

Les indicateurs listés dans ce chapitre sont les indicateurs proposés par le GRIVES. Il est fortement recommandé de suivre l'un ou l'autre des indicateurs proposés.

Les indicateurs suivis dans la structure sont les suivants *(supprimer de la liste les indicateurs non suivis, rajouter éventuellement des indicateurs suivis qui ne seraient pas listés)* :

- taux de formation du personnel par grandes catégories professionnelles ;
- taux de formation du personnel par catégorie spécifique de personnels.

4. Évaluation et amélioration des pratiques professionnelles

Les audits listés dans ce chapitre sont les audits proposés par le GRIVES. Il est fortement recommandé de réaliser annuellement au moins un audit relatif à l'identification primaire et un audit relatif à l'identification secondaire.
Le GRIVES, en accord avec l'ARS identifie chaque année, des audits à réaliser prioritairement. Ces audits font l'objet d'une exploitation régionale permettant ainsi un parangonnage entre établissement.

L'établissement prévoit dans son plan d'action annuel les audits à mettre en œuvre, a minima un audit relatif à l'identification primaire et deux audits relatifs à l'identification secondaire *(l'établissement modifie le nombre d'audits en fonction de ses pratiques)*.
L'établissement transmet les résultats des observations au GRIVES en vue d'une exploitation régionale permettant un parangonnage.
Les audits pouvant être réalisés sont les suivants.

Intitulé de l'audit	Complet	Flash
IDENTIFICATION PRIMAIRE		
Vérification de l'identité de l'usager (secrétariats sans création d'identité)	✔	✔
Recueil de l'identité lors de l'accueil de l'usager (points de création d'identité)	✔	✔
IDENTIFICATION SECONDAIRE		
Evaluation des règles d'identification lors d'un prélèvement biologique	✔	✔
Exhaustivité du port du bracelet d'identification chez le patient hospitalisé ou en ambulatoire	✔	
Evaluation des règles d'identification de l'usager lors d'un transport interne	✔	✔
Evaluation des règles d'identification de l'usager en imagerie médicale	✔	
Evaluation de l'identification des préparations injectables		✔
Identification de l'usager au moment de l'administration médicamenteuse		✔
Identification de l'usager lors du soin repas		✔

L'exploitation des audits est réalisée par le GRIVES au niveau régional et par le service qualité gestion des risques pour l'établissement.

L'analyse est présentée au *COSTRATIV au COMIV (la structure choisit le terme adapté en fonction du nom de l'instance de gouvernance (structures appliquant le RNIV2 ou structure éligible à appliquer le RNIV 3)*, accompagnée de propositions d'actions d'amélioration si nécessaire.

Les actions d'amélioration sont validées par le COSTRATIV *ou le COMIV (RNIV3)* et mises en œuvre par le référent en identitovigilance, la COIV, le service qualité gestion des risques. Les résultats sont restitués au personnel et disponibles dans la GED.

LA GESTION DES RISQUES

Objet du chapitre : ce chapitre vise à décrire les mesures mises en œuvre par l'établissement afin de gérer les risques à priori et a posteriori

1. La gestion des risques a priori

a) La veille réglementaire et technique.

Objectif du chapitre : décrire les actions de veille réalisées par le référent en identitovigilance.
*L'établissement adapte la rédaction proposée à ses pratiques. Il est fortement conseillé de mentionner les items identifiés par une *.*

Le référent en identitovigilance réalise une veille réglementaire et technique en utilisant les ressources disponibles (liste non exhaustive :

- journal officiel et bulletins officiels, lettre de l'APM, Hospimedia…** ;
- utilisation de l'espace collaboratif GRIVES ;
- consultation du site de l'Agence du Numérique en Santé ;
- communication des éditeurs ;
- participation des sessions de formations et d'information organisées par le GRIVES ;
- participation aux journées d'échanges et de partage organisées en région PACA ; à des manifestations nationales sur le thème de l'identitovigilance…

b) Modalités d'attribution et de gestion des droits d'accès informatiques

Objet du chapitre : préciser les principes retenus par la structure pour sécuriser les opérations de création, recherche, modification d'identités (qui détermine les droits ; comment sont formés et gérés les nouveaux arrivants, les intérimaires, les personnels qui quittent définitivement la structure…).

Dans la mesure du possible, il est conseillé aux établissements de mettre en œuvre une grille d'évaluation et de tracer l'évaluation réalisée dans le dossier RH du personnel par exemple, dans le cadre de la formation initiale et continue.

L'établissement a défini des profils d'accès au système d'informations dépendant de la fonction des personnels. La liste de ces profils est consultable dans la GED. Une attention particulière a été portée à la gestion des copies de pièces d'identité disponibles dans la GED. Seuls les personnels en charge de la création et de la fiabilisation des identités peuvent accéder à ces documents.
Les profils d'accès sont révisés annuellement par *mettre ici l'instance en charge de la révision des profils d'accès (commission profil et droit d'accès, médecin DIM…).*

L'attribution de droits d'accès au système d'information, la gestion des accès et les modalités de contrôles mises en œuvre sont décrites dans la charte informatique.
Si l'établissement dispose d'un annuaire de gestion des droits d'accès (type annuaire d'entreprise ou IAM), il peut être utile de le préciser ici.

Extrait du RNIV 2 : Une charte informatique formalisant les règles d'accès et d'usage du système d'information, et en particulier pour les applications gérant des données de santé à caractère personnel, doit être élaborée au sein de l'établissement (cf. Exi PP 13 RNIV 1). Validée par le niveau stratégique d'identitovigilance de la structure, elle formalise notamment la politique d'habilitation et les droits individuels attribués aux professionnels (…) ainsi que les modalités d'enregistrement des accès aux dossiers et des modifications effectuées. Elle doit être régulièrement actualisée (prérequis HOP'EN 3.2) et diffusée aux professionnels présents ainsi qu'aux nouveaux arrivants et, si cela est pertinent, aux prestataires et sous-traitants.

L'obtention de droit d'accès au système d'information est conditionnée par la signature de la charte d'utilisation des moyens informatiques.
Cette charte précise les droits et devoirs de l'utilisateur, répertorie l'ensemble des moyens informatiques et outils numériques mis à disposition des utilisateurs, définit les pratiques autorisées, les mesures de contrôle pouvant être mises en œuvre, les sanctions encourues en cas de non-respect des obligations de la charte.

Décrire ici l'organisation mise en œuvre pour gérer les droits d'accès et les habilitations ou renvoyer à la charte informatique ou à la procédure de sécurité informatique.
Par exemple :

Tout départ de personnel est signalé au service *mettre ici le nom du service compétent* le compte est alors immédiatement inactivé
Conformément à la politique générale de sécurité des systèmes d'information en santé, une revue des droits d'accès est réalisée semestriellement.
La liste des droits d'accès, la matrice des droits sont tenues à jour par le responsable des systèmes d'information.

Les personnels habilités à créer des identités sont formés et évalués avant l'attribution des droits.

c) Traçabilité des actions

Objet du chapitre : préciser les modalités d'analyse de l'historique des actions relatives aux données d'identité.

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.
L'accès à l'historisation des informations est limité aux personnels ayant besoin d'en connaître :
La structure définit les personnels ayant besoin d'accéder à l'historisation des informations. L'octroi de ces droits d'accès doit être justifié par la finalité (à préciser si des accès sont donnés à des fonctions qui peuvent paraître inhabituelles).
Préciser ici les fonctions des personnels autorisés par exemple :

- membre de la cellule opérationnelle d'identitovigilance
- service d'information médicale
- référent en identitovigilance
- personnels du service informatique…

Préciser ici les modalités de contrôle des accès par exemple :
Des contrôles d'accès aux dossiers sont réalisés :

- aléatoirement de façon semestrielle ;
- ponctuellement sur les dossiers sensibles (dossier de personnels de l'établissement, dossier de personnalités…) ou en cas de plainte ou de réclamation ou 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.

d) Fiabilisation des interfaces d'identités

L'établissement met en œuvre une procédure de test des interfaces d'identités. Ces tests sont conduits par la COIV, le service informatique et les référents logiciels métiers 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.

(si l'établissement ne dispose pas de base de tests, les tests doivent être conduits avant la remise à disposition des applicatifs pour les utilisateurs, l'établissement précise ici son organisation).
La procédure doit décrire qui est en charge de la réalisation des tests, à quelles occasion les tests sont réalisés, quels sont les tests réalisés, quelle est la traçabilité.

e) Sécurisation de l'identité dans les logiciels non ou incomplètement interfacés

(Ce chapitre doit être présent si les structures ne disposent pas d'un référentiel unique d'identité pour toutes les applications participant au processus de soin)

Objet du chapitre : décrire les mesures organisationnelles et techniques mises en place pour s'assurer que malgré l'absence d'interface ou la présence d'interfaces incomplètes, la même identité est utilisée pour le même usager dans tous les applicatifs
Exemple de mesure pouvant être mise en place :

- *réalisation d'un contrôle périodique de la cohérence des bases identités (logiciel d'identitovigilance permettant la comparaison des bases ;*
- *circuit de transmission de l'information éprouvé pour répercuter les fusions, les décollisions, les modifications de l'identité…*

f) Détection des utilisations frauduleuses d'identités

Objet du chapitre : faire un focus sur le risque d'utilisation frauduleuse d'identité. Ce chapitre est intéressant pour les établissements à risque (service des urgences, usagers en situation de précarité sociale).

L'établissement 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 usurpation d'identité. Les usagers sont sensibilisés aux risques encourus lors de l'utilisation frauduleuse d'une identité (affiches présentes aux points d'accueil).
L'établissement suit la recommandation ES05 du RNIV 2 et a fait le choix de signaler automatiquement une utilisation frauduleuse d'identité aux autorités judiciaires et à l'assurance maladie (*phrase à supprimer si ce n'est pas une pratique de la structure).*

La conduite à tenir devant une suspicion est formalisée et connue des personnels.

Pour mémoire (extrait du RNIV 2) : 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 (cf.* ***Error! Reference source not found.****) ;*
- *l'identification des documents transmis qui n'appartiennent pas à l'usager ;*
- *l'information des structures et professionnels avec lesquels les données ont été partagées ;*
- *la suppression de ces documents dans l'outil de partage virtuel utilisé par la structure (si applicable) ;*
- *la recherche de compléments d'informations ;*
- *le signalement externe aux parties prenantes (exemples : main courante, dépôt de plainte, alerte adressée à l'Assurance maladie, au médecin traitant, aux sous-traitants, information de l'usager dont l'identité a été empruntée…).*

2. La gestion des risques a posteriori

Objet du chapitre : préciser le dispositif mis en œuvre pour gérer les signalements des événements indésirables en relation avec l'identitovigilance. L'établissement adapte la rédaction proposée en fonction de son organisation et de ses pratiques.
Il est obligatoire de conduire une analyse des EIG.

L'établissement met en œuvre un système de signalement des événements indésirables, piloté par le service qualité gestion des risques. 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 usagers. L'établissement communique également auprès de ses partenaires *(préciser ici les principaux*

partenaires de l'établissement sous-traitants, établissements partenaires, médecins traitants, autres professionnels de santé) pour qu'ils lui signalent les anomalies constatées sur l'identification des usagers.

Les évènements indésirables graves font systématiquement l'objet d'une analyse utilisant une méthodologie adaptée (*préciser ici la méthode mise en œuvre ALARM…).* Les évènements porteurs de risques récurrents sont également analysés en comité de retour d'expérience.

Le référent en identitovigilance et la COIV sont informés de la survenue d'évènements indésirables, et destinataires des fiches de signalement. Ils participent à leur cotation, leur analyse, à la définition du plan d'action mis en place et à la mise en œuvre des actions.
Les évènements indésirables graves sont signalés sur le portail national de signalement des événements sanitaires indésirables.

Les évènements indésirables signalés, leur analyse permettent de réactualiser périodiquement (*mettre ici la périodicité de réactualisation*) la politique d'identitovigilance de l'établissement.

La formation et la sensibilisation des acteurs

Objet du chapitre : décrire les modalités de formation et de sensibilisation des professionnels.
Le texte proposé est une base indispensable à compléter par l''établissement

Tous les personnels de la structure sont formés à l'identitovigilance. La formation est obligatoire pour tous les nouveaux arrivants.
La formation dispensée comprend les éléments suivants :

- présentation de la gestion documentaires (principales procédures et organisation de la gestion documentaire) ;
- formation aux bonnes pratiques d'identitovigilance
    - identitovigilance secondaire avec base d'identitovigilance primaire pour le personnel soignant ;
    - identitovigilance primaire renforcée avec bases d'identitovigilance secondaire pour les professionnels de l'accueil secrétaires médicales, admissionnistes..) ;
- gestion des risques *a priori* avec en particulier une présentation des principaux risques identifiés dans l'établissement ;
- 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 évènements indésirables).

La formation des étudiants (*lister ici les catégories d'étudiants formés en ayant à l'esprit que la formation des internes est indispensable)* est organisée par la COIV en collaboration avec le comité pédagogique.
Les supports de formation sont produits par la COIV et validés par le COSTRATIV.

La formation est tracée : *préciser ici les modalités de traçabilité de la formation, idéalement émargement, tenue d'un listing des personnels formés et traçabilité dans le dossier de formation de chaque personnel*). Pour mémoire le taux de personnel formé fait partie des indicateurs d'identitovigilance.

Le plan de formation continue de l'établissement intègre les formations en lien avec l'identitovigilance.
Les personnels suivent une formation de remise à niveau tous les trois ans.
L'établissement décrit ici les modalités d'organisation des sessions de formation par exemple :
3 sessions de formation à l'identification secondaire et 2 sessions de formation à l'identification primaire sont organisées annuellement. la formation est dispensée par un personnel de la COIV. Les dates sont communiquées aux cadres des services, qui alimentent un fichier d'inscription. Il est obligatoire d'assister à au moins une session tous les trois ans.

Si de mauvaises pratiques du fait d'un professionnel sont identifiées, un point personnalisé est réalisé par la COIV en présence du responsable hiérarchique si cela est nécessaire.

3. Action de sensibilisation et de communication auprès des professionnels

Ce chapitre vise à présenter les actions de communication et de sensibilisation menées
Des actions de sensibilisation sont menées dans l'établissement : *lister ici les actions menées :*

- au cours de la semaine de sécurité des soins (jeux chambre des erreurs…) ;
- affichage dans les services de posters ;
- distribution de flyers de sensibilisation ;
- communication autours des erreurs, des presque accidents ou évènements porteurs de risques, analyse des évènements indésirables…

RESPECT DES DROITS DE L'USAGER, INFORMATION SENSIBILISATION

1. Respect du RGPD

Objet du chapitre : préciser les modalités mises en œuvre par la structure pour la mise en conformité du traitement des données personnelles informatisées avec le règlement général de protection des données.
Exemple de rédaction :
Le *CH mettre ici le nom de l'établissement* a formalisé, sous l'autorité de son délégué à la protection des données (DPD), 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 (*à conserver si l'établissement utilise ou alimente des services régionaux, via trajectoire, e parcours ou télémédecine, dossier communicant de cancérologie..)*.
Un document d'information sur l'utilisation de ces services est affiché dans les lieux d'accueil administratif et dans le livret d'accueil de l'établissement. Il 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'usager. Ce document rappelle en particulier les droits de l'usager :

- d'être informé en cas de traitement automatisé des informations le concernant en particulier 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);
- d'avoir accès aux informations médicales le concernant ;
- de demander la rectification des données erronées ou périmées ;
- d'avoir la garantie de la confidentialité des informations le concernant…

Une fiche pratique proposée par le 3RIV est disponible pour vous aider à rédiger les documents d'information de l'usager.

2. Information et sensibilisation des usagers

Objet du chapitre : préciser les modalités d'information des usagers sur l'identitovigilance primaire et secondaire et en particulier sur la gestion de leurs données d'identité. L'établissement modifie/complète ce chapitre selon les moyens de communication disponibles dans la structure.

L'établissement accorde une attention particulière à l'information des usagers qui doivent être acteurs de leur parcours de soins.
L'information est réalisée par le biais d'affiches traitant d'identification primaire disposées dans les points d'accueil et d'affiche traitant d'identification secondaire disposées dans les services de soins et au centre de consultations. Le livret d'accueil de l'usager hospitalisé intègre un chapitre concernant la gestion de l'identité et ses droits d'accès et de modification de ses données.
L'identitovigilance est abordée lors des réunions de la commission des usagers.
La semaine de sécurité des usagers *(la structure précise ici les périodes au cours desquelles elle conduit des actions spécifiques de sensibilisation)* est mise à profit pour organiser des ateliers spécifiques identitovigilance à destination des usagers.

L'usager est informé au plus tôt des documents qu'il devra présenter lors de sa venue en particulier un dispositif d'identification à haut niveau de confiance :

- les éléments d'information sont présents sur les affiches, dans le livret d'accueil ;
- ils sont présents sur l'outil de prise de rendez-vous en ligne et de préadmission en ligne ;
- ils sont envoyés dans les mails de confirmation de prise de rendez-vous en ligne…

Actualisation de la charte et de la politique d'identitovigilance

Objet du chapitre : préciser les modalités de réactualisation de la charte et de la politique.

La politique et la charte sont actualisées périodiquement *(mettre ici la périodicité de révision)* pour prendre en compte :

- les évolutions réglementaires ;
- les résultats des évaluations menées dans l'établissement et les résultats des indicateurs ;
- les évènements indésirables, leur analyse, les plans d'actions mis en place.

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
- 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 certification des établissements de santé pour la qualité des soins. Octobre 2020
    - 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

Annexe 1 : proposition de gouvernance pour groupements

Objet de l'annexe : cette annexe est destinée à remplacer le chapitre III si ce modèle est utilisé pour rédiger une charte d'identitovigilance de groupement

1. Le comité stratégique d'identitovigilance (COSTRATIV) du *GHT ou groupement indiquer ici le nom de la structure.*

a) Composition

A minima, chaque établissement partie ou associé au GHT doit être représenté par le référent d'identitovigilance de l'établissement et le responsable qualité ou le coordonnateur de la gestion des risques associés aux soins.
Le DIM de Territoire est obligatoirement membre de la cellule d'identitovigilance territoriale.
Il est fortement conseillé de ne pas identifier les membres nominativement dans la charte et de prévoir annuellement une note de désignation nominative signée par le directeur du GHT ou du groupement (ceci permet de ne pas devoir revoir la charte à chaque changement d'un membre).

Ce COSTRATIV s'appuie sur les instances décisionnaires et opérationnelles de chaque établissement (voir infra).

Le COSTRATIV est représentatif de toutes les structures participant au *GHT/groupement*.

Décrire ci-dessous la liste des membres de la COSTRATIV et l'organisation mise en place ou renvoyer à une note d'organisation. la composition proposée ici est minimale, les GHT ou groupements peuvent la compléter par exemple par les responsables des bureaux des entrées, les responsables ou directeurs des systèmes d'information.

- Responsable de la CIV de GHT ou de groupement :
    - Etablissement 1 :
        - Référent en identitovigilance,
        - Responsable qualité ou coordonnateur de la gestion des risques associés aux soins,
    - Etablissement 2 :
        - Référent en identitovigilance,
        - Responsable qualité ou coordonnateur de la gestion des risques associés aux soins,
    - Etablissement n :
        - Référent identitovigilance,
        - Responsable qualité ou coordonnateur de la gestion des risques associés aux soins,
- DIM de GHT ou de groupement :
- Président de la CME de GHT ou de groupement
- Pilote de l'instance qualité du groupement ou du GHT

b) Missions

Les missions du COSTRATIV sont les suivantes :
- définir la politique d'Identitovigilance du groupement ou du GHT et décliner son plan d'actions annuel ;
- veiller à la cohérence des chartes politiques et pratiques des établissements avec les politiques, charte et procédures du groupement ou du GHT
- définir la politique de formation et de communication en termes d'Identitovigilance pour le groupement ou le GHT et s'assurer de sa mise en œuvre au sein des établissements partie ou associés au groupement ;
- mettre en place un système d'évaluation et de suivi qualité (indicateurs, audits, suivi et analyse des évènements indésirables liés à l'identification de l'usager pour ceux concernant les interfaces entre établissements…) ;

- définir le besoin en documents qualité (procédures, modes opératoires…) pour le groupement ou le GHT et s'assurer de la mise en place d'une gestion structurée de la documentation relative à la politique d'identification des usagers au sein des établissements partie ou associés au GHT ou au groupement ;
- s'assurer de la bonne application des procédures concernant les identifications et les bonnes pratiques professionnelles, conformément à la réglementation et aux recommandations, régionale, du groupement ou du GHT ;
- participer à l'analyse des risques *a priori* du groupement ou du GHT concernant l'identification de l'usager à toutes les étapes de sa prise en charge ;
- Collecter, analyser et résoudre les problématiques du groupement ou du GHT liées aux actions d'identification et en particulier aux problématiques d'interfaces entre deux établissements ;
- Participer à la définition d'une architecture cible du système d'identification du patient au sein du groupement ou du GHT ;
- Rendre compte aux instances stratégiques du groupement ou du GHT.

Les groupements ou GHT adapteront les missions proposées ci-dessus en fonction de leur organisation.

Le fonctionnement de l'instance stratégique est régi par un règlement intérieur.

c) Fréquence de réunion

L'instance décisionnaire du groupement ou de GHT se réunit *a minima* une fois par semestre. Chaque réunion donne lieu à un compte rendu formalisé et diffusé à chaque établissement participant au groupement.

2. Le référent en identitovigilance du GHT ou du groupement

Le référent en identitovigilance du GHT ou du groupement est nommé par le comité stratégique du GHT ou du groupement sur proposition des membres de la cellule d'identitovigilance territoriale. Il est désigné via une note de nomination cosignée par le directeur du GHT ou du groupement et le président de la CME du GHT ou du groupement.

Prévoir une note de désignation nominative à révision annuelle et une lettre de mission.

Les missions proposées ici complètent les missions d'un référent local
Le référent en identitovigilance du GHT ou du groupement :

- est membre de droit du comité stratégique territorial d'identitovigilance ;
- est l'interlocuteur privilégié du comité stratégique de groupement ou de GHT de l'ensemble du personnel pour toutes les problématiques liées à l'identification de l'usager (identification primaire et secondaire) ;
- organise le fonctionnement de la cellule d'identitovigilance territoriale ;
- planifie et anime les réunions ;
- est l'interlocuteur privilégié du comité stratégique, de la CME du GHT ou du groupement, des instances décisionnaires des établissements et des référents locaux d'identitovigilance des établissements ;
- veille à la réalisation de l'ensemble des missions de la cellule d'identitovigilance territoriale (cf. mission COSTRATIV) ;
- participe au réseau régional du GRIVES PACA.

3. La cellule opérationnelle d'identitovigilance du groupement ou du GHT

Selon les organisations adoptées, le groupement peut choisir :

1. *de mettre en place une instance opérationnelle de groupement, en charge de réaliser les rapprochements d'identités, de traiter au quotidien les problématiques partagées entre plusieurs établissements. Cette instance opérationnelle sera alors constituée de personnels aguerris dans la gestion de l'identité et de ses problématiques (techniciens*

d'informations médicales, Assistants médico-administratifs référents spécifiquement formés) et d'un expert (médecin DIM, biologiste médical, pharmacien hospitalier…) reconnu pour ses compétences en identitovigilance).

2. *de s'appuyer sur les instances opérationnelles des établissements partie ou associés.*

Décrire ici le mode de fonctionnement choisi par le GHT ou le groupement.

a) Composition

Décrire la composition de la cellule et le mode de fonctionnement (subordination hiérarchique, technique…). Préciser les ETP dédiés

b) Missions

Si la cellule a des missions spécifiques (non présente dans les missions des cellules opérationnelle d'identitovigilance locales, décrire ici les missions spécifiques.

Annexe 2 : proposition de gouvernance pour les établissements sanitaires bénéficiant de la mesure dérogatoire leur permettant d'appliquer le RNIV 3

Objet de l'annexe : cette annexe est destinée à remplacer le chapitre III si le modèle de charte est utilisé pour rédiger une charte d'identitovigilance au profit d'un établissement sanitaire bénéficiant de la mesure dérogatoire lui permettant d'appliquer le RNIV 3.
Le comité d'identitovigilance peut être compris dans le comité qualité ou le comité de direction de l'établissement. Il n'est pas nécessaire de disposer d'une instance spécifique à condition que les problématiques d'identitovigilance soient traitées à chaque réunion de l'instance.

1. Le comité d'identitovigilance (COMIV) du *CH indiquer ici le nom de la structure.*

a) Composition

La composition du COMIV est la suivante :
- le directeur ou son représentant ;
- un représentant du corps médical ;
- un représentant du corps paramédical ;
- le médecin de l'information médicale (DIM) ou son représentant ;
- le responsable de la cellule qualité gestion des risques (CQGR) ou son représentant ;
- le référent en identitovigilance ou son représentant ;
- le directeur ou le responsable des systèmes d'information (RSI) ou son représentant ;
- le délégué à la protection des données (DPD) de la structure ;
- le responsable des admissions ;
- un représentant des structures partenaires (sous-traitants et prestataires) ;

La composition du COMIV est actualisée annuellement et est disponible dans la gestion documentaire (*indiquer ici le nom de la GED*).

b) Missions

Les missions du COMIV sont les suivantes :

- définir la politique d'Identitovigilance de l'établissement et décliner son plan d'action annuel *en veillant à la cohérence des documents de l'établissement avec les documents du groupement ou du GHT ;*
- arrêter l'organisation à mettre en œuvre (instances, missions confiées) ;
- définir les moyens humains, techniques et financiers à attribuer pour le fonctionnement optimal de cette organisation ;
- définir la politique de formation en identitovigilance conduite dans l'établissement *en cohérence avec la politique définie par l'instance du groupement ou GHT*, et s'assurer de sa mise en œuvre ;
- mettre en place un système d'évaluation et de suivi qualité (indicateurs, audits, suivi et analyse des évènements indésirables liés à l'identification de l'usager…) *en cohérence avec celui défini dans le groupement* ;
- s'assurer de la bonne gestion des documents qualité relatifs à l'identification de l'usager au sein de l'établissement *et de leur cohérence avec les documents qualité communs au groupement* ;
- participer à la gestion des risques en identitovigilance :
  - gestion des risques *a priori* : cartographie des risques de l'établissement,
  - gestion des risques *a posteriori* : suivi des évènements indésirables et actions correctives, préventives ou d'atténuation à mettre en œuvre ;
- s'assurer de la bonne application des procédures concernant l'identification et les bonnes pratiques professionnelles, conformément à la réglementation *et aux recommandations du groupement ou du GHT* ;
- collecter, analyser et résoudre les problématiques locales liées aux actions d'identification ;

- alerter la direction de l'établissement sur les éventuels problèmes ou dysfonctionnements dans la mise en œuvre de la politique et/ou de la charte d'identitovigilance ;
- *alerter l'instance décisionnaire du groupement ou du GHT sur des problèmes survenant aux interfaces de deux établissements partie ou associés au groupement*
- signaler des événements indésirables graves en rapport avec l'identification des usagers sur le portail de signalement des évènements sanitaires indésirables ;
- formaliser 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 ;
- 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 ;
- participer à la formation continue des soignants en charge de l'identification secondaire ;
- rédiger et actualiser les documents qualité relatifs à l'identification primaire ou secondaire de l'usager ;
- maintenir la qualité de la base patient locale en résolvant les problèmes liés à l'identification primaire (fusion de doublons, défusion de collision…) ;
- contrôler la qualité des bases de données utilisées par la structure ;
- *contribuer au rapprochement d'identité entre établissement en statuant sur les identités proposées au rapprochement inter établissement (si l'établissement participe à un rapprochement d'identités) ;*
- recueillir et analyser les évènements indésirables en lien avec l'identitovigilance en collaboration avec le service qualité gestion des risques ;
- recueillir et analyser les indicateurs qualité.
- *communiquer annuellement le bilan d'activité à l'instance décisionnaire du groupement ou du GHT*.

Un règlement intérieur régi le fonctionnement du COMIV.

c) Fréquence de réunions

Le COMIV se réunit au moins deux fois par an.
Point d'attention : les missions opérationnelles sont réalisées au fil de l'eau par les personnels en charge.

2. Le référent en identitovigilance

Objet du chapitre : préciser les missions du référent en identitovigilance de la structure.

Le référent local en identitovigilance est désigné par le directeur de l'établissement et le président de la CME (cf. note de désignation présente dans la gestion documentaire *mettre ici le nom de la GED*).
Point d'attention : il est fortement préconisé que le référent en identitovigilance de la structure soit identifié dans le répertoire opérationnel des ressources (ROR). Il doit disposer de la compétence particulière « identitovigilance » sur sa fiche professionnelle.

L'établissement complète les missions du référent en identitovigilance si nécessaire.

- Le référent en identitovigilance de l'établissement / *du groupement ou du GHT* est membre de droit du comité stratégique d'identitovigilance de l'établissement (COSTRATIV).
- *Il participe au comité stratégique d'identitovigilance territorial.*
- Il assure la supervision technique des activités de la cellule opérationnelle d'identitovigilance (COIV).
- Il organise l'identitovigilance au sein de l'établissement / *du groupement ou du GHT* conformément aux exigences règlementaires (RNIV) et aux bonnes pratiques d'identitovigilance.
- Il est l'interlocuteur privilégié de la direction de l'établissement, de la CME, *du comité stratégique de groupement ou de GHT* de l'ensemble du personnel pour toutes les problématiques liées à l'identification de l'usager (identification primaire et secondaire).

- Il participe à l'élaboration de la politique d'identification des usagers en lien avec la direction, la CME et le COSTRATIV, le coordonnateur de la gestion des risques associés aux soins, le directeur ou le responsable qualité de l'établissement.
- Il organise et/ou anime les réunions du COSTRATIV.
- Il assure la veille réglementaire et technique en matière d'identitovigilance.
- Il s'assure de l'adéquation des pratiques avec les exigences de l'identitovigilance.
- Il participe à l'élaboration des plans de crise en particulier l'organisation de l'identification des victimes.
- Il contribue aux travaux de convergence des systèmes d'information du GHT ou du groupement mettre ici le nom du groupement auquel appartient mettre ici le nom de la structure en matière d'identitovigilance ;
- Il participe au choix des outils et donne un avis d'expert sur leur conformité aux exigences des référentiels (RNIV, guide d'implémentation de l'INS…) et leur adéquation aux besoins de la structure en termes d'identification de l'usager.
- Il supervise le suivi (rédaction, révision) des documents qualité (procédures, modes opératoires, fiches réflexes…) nécessaires à l'organisation et au suivi de l'identitovigilance au sein de l'établissement.
- Il participe à la gestion des risques *a priori* et *a posteriori*.
- Il élabore ou s'assure de l'élaboration du plan d'actions annuel et de son suivi et établit le rapport annuel d'activités.
- Il définit, en lien avec le COSTRATIV, le service qualité, le coordonnateur de la gestion des risques associés aux soins, la cellule opérationnelle d'identitovigilance, le planning annuel des évaluations, s'assure de leur réalisation et participe à l'analyse des résultats et à la définition des plans d'actions et de leur mise en place.
- Il s'assure de la formation et de la sensibilisation du personnel en matière d'identitovigilance, en particulier, des règles de vérification de l'identité des usagers en lien avec le service formation continue de l'établissement.
- Il supervise le maintien de la qualité du référentiel identité de l'établissement en particulier de la détection et du traitement des doublons potentiels, de la gestion des collisions, des anomalies liées à l'INS.
- Il est responsable de la diffusion et de la gestion des alertes d'identitovigilance internes et externes dans son établissement.
- Il assure le suivi des indicateurs d'identitovigilance définis au niveau de l'établissement et leur analyse.
- Il assure le suivi des déclarations des évènements indésirables relatifs à l'identification de l'usager et participe à leur analyse et à la mise en place d'actions d'amélioration.
- Il assure, dans le cadre de la procédure de certification, l'évaluation du critère 2.3-01 « les équipes respectent les bonnes pratiques d'identification du patient à toutes les étapes de sa prise en charge ».
- Il assure la communication interne et externe autours de l'identitovigilance :
    - vers la commission des soins infirmiers, de rééducation et médico-techniques (CSIRMT), Commission médicale d'établissement…),
    - vers des instances régionales,
    - vers les personnels de l'établissement,
    - *vers les instances de groupement ou de GHT*.
- Il participe au réseau régional du GRIVES.

Il rend compte à la direction de l'établissement et à la CME de l'ensemble de ses activités, de toute difficulté rencontrée et des problématiques relatives à l'identitovigilance survenant dans son établissement.