

IDENTITOVIGILANCE
NOUVELLE-AQUITAINE

**Comité technique régional d'identitovigilance
de Nouvelle-Aquitaine**

**MODÈLE RÉGIONAL
DE CHARTE
D'IDENTITOVIGILANCE
DES ÉTABLISSEMENTS
SANITAIRES
ET MEDICO-SOCIAUX**

Juin 2019

Liste des contributeurs

Dr Bérénice BRECHAT-HUET, CH Cadillac

Mme Céline DESCAMPS, CRIV

Dr Béatrice JANVOIE-OUILLET, GH La Rochelle-Ré-Aunis

Dr Nadia KHALDI, EFS NAQ

Mme Christelle NOZIERE, CRIV

Mme Sylvie OUAZAN, CH Pau

Mme PERREAUD Nathalie, CH Arcachon

Dr Bernard TABUTEAU, ARS NA

Mme Françoise URSULET, CRIV

PREAMBULE

Une charte est un document officiel destiné à établir des objectifs, des valeurs, des principes ou des règles partagées.

Dans le monde de la santé, elle est utilisée pour définir des engagements pris par les signataires vis-à-vis des usagers (charte de la personne hospitalisée, charte du parcours patient, charte de promotion de la santé...) ou des professionnels (charte de la visite médicale, charte de confiance pour le signalement des événements indésirables...).

La charte d'identitovigilance est un document qui a pour objet de formaliser la politique de chaque structure de santé en matière d'identification des usagers pris en charge. Elle définit le périmètre et les conditions d'enregistrement, d'utilisation et de sécurisation des données d'identité ainsi que l'information des parties prenantes. Elle fait référence aux documents spécifiques qui développent les aspects techniques et opérationnels : procédures, protocoles, modes opératoires...

Afin d'harmoniser les différentes chartes existantes et de s'assurer de leur conformité avec le *référentiel régional de bonne pratique* en vigueur¹, le *Comité technique régional d'identitovigilance* (COTRIV) de Nouvelle-Aquitaine met à disposition des structures de santé un modèle de charte. Ce document type, qui rappelle les éléments à retrouver de façon obligatoire dans la charte, est à adapter par chaque structure de santé en fonction de ses spécificités organisationnelles et techniques.

MODE D'EMPLOI

Le présent document fixe le modèle de charte d'identitovigilance que le COTRIV préconise d'utiliser en Nouvelle-Aquitaine. On y retrouve un plan général de présentation ainsi qu'une aide constituée, pour chaque chapitre :

- d'un commentaire sur l'objet du chapitre ;
- d'un exemple de rédaction de contenu dans une situation fictive avec un établissement dénommé « SSAN » utilisant un serveur d'identités appelé « GAMMA ».

Pour formaliser la charte locale d'identitovigilance de leur structure d'appartenance, les professionnels sont invités à :

- conserver le plan du document ;
- modifier l'exemple proposé en tant que besoin afin qu'il décrive parfaitement la politique, l'organisation, les documents et les pratiques en vigueur au niveau local ;
- supprimer, à la fin du processus, les éléments d'aide *en police italique marron*.

¹ <https://www.nouvelle-aquitaine.ars.sante.fr/lidentitovigilance-au-coeur-de-la-securite-des-soins>

STRUCTURE GENERALE

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

1. Introduction
2. Politique d'identitovigilance
 21. Définition et objectifs
 22. Engagement de la structure
 23. Gouvernance
 24. Périmètre
 25. Respect du RGPD
3. Eléments d'identification
 31. Terminologie
 32. Traits d'identification
 33. Domaines d'identification et de rapprochement
 34. Confiance dans les identités gérées
 35. Identités particulières
4. Gestion des risques *a priori*
 41. Gestion documentaire
 42. Gestion des habilitations
 43. Traçabilité des actions
 44. Information des usagers
 45. Formation et sensibilisation des acteurs
5. Gestion des risques *a posteriori*
 51. Gestion documentaire
 52. Déclaration et gestion des événements indésirables
 53. Gestion d'une erreur d'identité
 54. Gestion des anomalies du domaine de rapprochement
 55. Indicateurs de suivi
6. Connexion au serveur régional de rapprochement (si applicable)
7. Références réglementaires et techniques

1 INTRODUCTION

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

Exemple de rédaction :

La présente charte d'identitovigilance a pour objet de formaliser la politique conduite par SSAN en matière d'identification des usagers pris en charge afin de garantir leur sécurité tout au long de leur parcours. Elle définit l'organisation et les moyens mis en œuvre ainsi que les règles à respecter par l'ensemble des professionnels de l'établissement. Elle traite également des droits et devoirs des usagers qui sont également pleinement parties prenantes de leur propre sécurité.

2 POLITIQUE D'IDENTITOVIGILANCE

2.1 Définition et objectif

Objet du chapitre : définir l'identitovigilance et décrire les objectifs de la structure en termes de bonnes pratiques d'identification des patients/usagers.

Exemple de rédaction :

La maîtrise de l'identification des usagers est un enjeu majeur pour garantir la qualité et la sécurité de leur prise en charge, notamment lors des actes de soins – qu'ils soient réalisés à titre préventif, diagnostique ou curatif. L'identitovigilance représente l'ensemble des moyens organisationnels et techniques mis en œuvre pour disposer d'une identification unique, fiable et partagée du patient afin d'éviter les risques d'erreurs tout au long de son parcours de santé.

Les règles d'identitovigilance s'imposent à l'ensemble des usagers du système de santé, qu'ils soient professionnels médicaux, paramédicaux, administratifs, ou patients. Elles sont un prérequis pour la sécurisation du partage d'informations de santé, qu'il soit réalisé au sein de la structure ou lors des échanges avec les référents médicaux du patient, dans le respect du secret médical.

2.2 Engagement de la structure

Objet du chapitre : préciser la politique mise en œuvre dans la structure en matière d'identitovigilance et rappeler son lien avec le Référentiel régional applicable.

Exemple de rédaction :

Dans le cadre de la démarche de management de la qualité intégrée à la gestion des risques conduite par SSAN, le processus d'identification des patients a été identifié comme un domaine porteur de risques *a priori*. Il a d'ailleurs été signalé des événements indésirables associés aux soins (EIAS) dont le principal facteur de survenue était un manque de contrôle de l'identité à certaines étapes de la prise en charge.

La direction de SSAN, en association avec les instances responsables de la qualité des soins et de la sécurité des usagers, entend conduire une politique d'identitovigilance forte qui a pour objectifs de :

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

Cette politique est définie en conformité avec les principes établis dans le *Référentiel de bonne pratique en matière d'identitovigilance en région Nouvelle-Aquitaine*, dans sa version mise à jour en décembre 2018.

2.3 Gouvernance

Objet du chapitre : préciser la structuration de l'identitovigilance en termes :

- *de conduite de la politique d'identitovigilance dans la structure ;*
- *de traitement des signalements d'erreurs constatées ;*
- *d'analyse et de correction des anomalies dans la base (doublons, fusions...).*

Exemple d'introduction du chapitre :

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

- le comité de pilotage de l'identitovigilance (COPILIV) ;
- la cellule locale d'identitovigilance (CLIV) ;
- les correspondants d'identitovigilance ;
- les référents logiciels.

2.3.1 Le comité de pilotage de l'identitovigilance (COPILIV)

Objet du chapitre : préciser la dénomination, le rôle et la composition du niveau décisionnaire.

Exemple de rédaction :

Le COPILIV a pour objet de définir les orientations de la politique d'identitovigilance et les moyens à mettre en œuvre pour la faire respecter. Il s'assure de la cohérence des différentes applications du système d'information, valide les documents publiés par la structure dans ce domaine. Il se tient informé des résultats obtenus et des difficultés rencontrées. Il contrôle la cohérence du plan de formation avec les objectifs de formation et de sensibilisation des différents acteurs concernés.

Les actions d'amélioration validées en COPILIV sont intégrées au programme d'amélioration de la qualité et de la sécurité (PAQSS) de SSAN.

La composition du COPILIV 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 de la cellule qualité gestion des risques (CQGR) ou son représentant ;
- le responsable de la cellule locale d'identitovigilance (CLIV) ou son représentant ;
- le responsable des systèmes d'information (RSI) ou son représentant.
- le délégué à la protection des données (DPD) rattaché à SSAN.

La liste actualisée des membres du COPILIV est disponible dans la gestion documentaire (GED, cf. 4.1).

Le COPILIV se réunit au moins une fois par an. Il transmet un bilan annuel au *Comité technique régional d'identitovigilance (COTRIV)* de Nouvelle-Aquitaine (§ 2.4.1 du *Référentiel régional*).

2.3.2 La cellule locale d'identitovigilance (CLIV)

Objet du chapitre : préciser les missions et la composition de la structure chargée de la conduite opérationnelle de l'identitovigilance dans la structure.

Exemple de rédaction :

La CLIV est l'instance opérationnelle de l'identitovigilance pour SSAN. 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 ;
- rédiger et/ou actualiser les procédures d'identitovigilance ;
- recueillir et analyser les événements indésirables en lien avec l'identitovigilance ;
- contrôler la qualité des bases de données utilisées par la structure ;
- recueillir et analyser les indicateurs qualité ;
- mettre en place les actions préventives et/ou correctives souhaitables ;
- informer le COPILIV des difficultés rencontrées.

La CLIV comprend les personnes suivantes :

- le médecin DIM, responsable de la CLIV ;
- le responsable de l'accueil et de la facturation ;
- un représentant de la DSI ;
- le responsable de la CQGR ;
- le coordonnateur de la gestion des risques associés aux soins (CoGRAS) ;
- un cadre de santé ;
- des correspondants d'identitovigilance ;
- des référents logiciels ;
- un représentant d'utilisateur.

La liste actualisée des membres de la CLIV est disponible dans la GED (cf. 4.1).

La CLIV se réunit au moins une fois par trimestre. Elle formalise un bilan périodique de ses activités, au moins annuel, qui précise les indicateurs suivis et leurs résultats, les incidents relevés et les mesures correctrices prises. Ces bilans sont transmis au COPILIV.

La CLIV est chargée de vérifier la mise en application des actions et de leur efficacité, en relation avec la CQGDR. Les indicateurs suivis, les objectifs à atteindre et les actions planifiées dans le PAQSS sont formalisés dans le rapport annuel de la CLIV transmis au COPILIV.

2.3.3 Correspondants d'identitovigilance

Objet du chapitre : préciser les missions des professionnels correspondants dans les services (si applicable).

Exemple de rédaction :

• Correspondants internes

Chaque service clinique et médicotechnique de SSAN désigne au moins un correspondant d'identitovigilance. Ces professionnels ont pour mission d'assurer le relais des décisions de la CLIV dans les différents secteurs d'activité. Ils sont également chargés de faire remonter les difficultés rencontrées par les acteurs de terrain.

Ils participent aux actions de formation et de sensibilisation de la structure en matière d'identitovigilance et peuvent être invités aux réunions de la CLIV. La liste des correspondants d'identitovigilance est affichée dans chaque service.

- **Correspondants externes**

Des correspondants d'identitovigilance sont également identifiés dans les structures partenaires (cabinet de radiologie RADIOSARL et laboratoire de biologie MEDILAB) qui ne font pas partie du domaine d'identification interne. Ils ont pour objet de faciliter la mise en commun des règles d'identitovigilance mais aussi de participer au signalement et au traitement des erreurs dans le cadre des données de santé échangées (domaine de rapprochement, cf. 3.3).

Ces référents sont invités à participer aux réunions de la CLIV pour les sujets qui les concernent.

La CLIV et les structures partenaires disposent chacun de la liste de l'ensemble des correspondants d'identitovigilance. Elle est mise à jour en tant que besoin dans la GED (cf. 4.1).

2.3.4 Référents logiciels

Objet du chapitre : préciser le rôle des référents logiciels.

Exemple de rédaction :

Le système d'information de la structure réunit plusieurs applications informatiques dédiées à des tâches spécifiques (cf. 3.3). Pour assurer la cohérence de l'ensemble des logiciels destinés à traiter des informations personnelles d'utilisateurs, chaque application est pilotée par un référent.

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

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

La CLIV dispose de la liste de l'ensemble des référents logiciels. Elle est mise à jour en tant que besoin dans la GED (cf. 4.1).

2.4 Périmètre

Objet du chapitre : préciser le périmètre d'application des règles d'identitovigilance locales.

Exemple de rédaction :

La politique d'identitovigilance s'applique au domaine d'identification de SSAN, c'est-à-dire à toutes les applications qui utilisent le référentiel d'identité patient GAMMA pour désigner les usagers. Le COPILIV s'assure que les autres domaines d'identification échangeant des données avec les applications de la structure (cf. 2.3.3 et 3.3) disposent également d'une politique d'identitovigilance compatible avec celle de SSAN.

2.5 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 :

La direction de SSAN a formalisé, sous l'autorité de son délégué à la protection des données (DPO), la documentation prévue par le règlement général de protection des données (RGPD), y compris pour l'utilisation de ces données dans le cadre de la connexion au serveur de rapprochement d'identités (SRI) régional (cf. 6).

Un document d'information sur le SRI est affiché dans les lieux d'accueil administratifs et dans le livret d'accueil de l'établissement (cf. 4.4). Il précise les modalités d'utilisation des données d'identité personnelles dans le cadre régional et du respect des volontés de l'utilisateur.

3 ELEMENTS D'IDENTIFICATION

3.1 Terminologie

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

Exemple de rédaction :

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

3.1.1 Identification

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

3.1.2 Identité et identifiant

Identité : représentation d'une personne physique du monde réel. L'identité est composée d'un identifiant et d'un profil de traits (cf. 3.1.4).

Identifiant : séquence de caractères qu'un ou plusieurs domaines d'identification (cf. 3.1.3) utilisent pour représenter une personne et lui associer des informations dans le cadre de sa prise en charge.

Au sein de SSAN, il est distingué plusieurs catégories d'identifiants :

- l'identifiant d'épisode patient (IEP) qui est créé pour chaque événement relatif au séjour du patient : c'est le numéro de séjour ;
- l'identifiant permanent patient (IPP) qui est créé pour chaque nouveau patient non encore connu de l'établissement. Chaque patient a donc un IPP unique², constant dans le temps, auquel sont rattachés les identifiants de venue ;
- l'identifiant national de santé (INS) qui correspond à son numéro d'inscription au registre (NIR) de l'INSEE. Chaque patient immatriculé en France (cela ne concerne donc pas les étrangers) possède donc un identifiant unique valable sur l'ensemble du territoire et dans toutes les structures de santé.

3.1.3 Domaine d'identification et de rapprochement

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

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

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

NB : le rapprochement entre 2 identités est également possible au sein d'un même DI ; il correspond à la recherche et au traitement des doublons (cf. 3.1.5).

3.1.4 Trait d'identification

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

En cohérence avec le référentiel régional d'identitovigilance, SSAN distingue 3 catégories de traits d'identification (cf. 3.2).

- Les **traits stricts** : ce sont des informations invariables dans le temps et requises de façon obligatoire pour identifier un patient de manière fiable et permettre un rapprochement.
- Les **traits étendus** : ce sont d'autres informations pouvant être utilisées pour faciliter le rapprochement d'identités entre 2 dossiers lorsque les éléments précédents ne sont pas suffisants ou lorsqu'il existe des doutes sur une possible usurpation d'identité. Leur saisie est hautement souhaitable, quand ils sont disponibles, car ces traits contribuent au rapprochement et à la recherche de doublons.
- Les **traits complémentaires** : ce sont des informations supplémentaires facultatives, potentiellement utiles pour consolider une identification ou un rapprochement d'identité.

3.1.5 Doublons, fusion, collisions

Le *référentiel régional d'identitovigilance* précise la définition d'un certain nombre de termes dans son glossaire (§ 8). Il n'en sera précisé que certains dans cette charte qui ont une importance toute particulière en termes de qualité et de sécurité de la prise en charge.

- Le **doublon d'identités** : il correspond à l'identification d'une même personne sous 2 identifiants différents dans un même domaine d'identification. Les informations d'un même patient sont donc réparties dans plusieurs dossiers différents qui ne communiquent pas entre eux et aboutit à la mise à disposition d'informations incomplètes.
- La **fusion** correspond au traitement des doublons ; elle consiste à regrouper toutes les informations d'un même individu sous un identifiant unique.
- La **collision** correspond au regroupement sous un même identifiant d'informations issues de 2 patients différents ; cela peut résulter d'une fusion réalisée avec des critères insuffisants ou bien d'une erreur de choix de dossier patient lors d'une venue. Ces situations de non-qualité sont particulièrement difficiles à corriger.

3.2 Traits d'identification

Objet du chapitre : préciser les traits d'identification et les règles d'enregistrement retenus dans la structure et leur cohérence avec les règles d'identitovigilance régionales opposables.

Exemple de rédaction :

Conformément au *référentiel régional d'identitovigilance*, SSAN classe les traits d'identification qu'il utilise selon 3 catégories (cf. 3.1.4). Une procédure interne définit comment sont retenus et vérifiés ces différents traits.

3.2.1 Traits stricts

- Nom de famille (ou nom de naissance)
- Premier prénom de naissance figurant sur le document officiel d'identité
- Date de naissance
- Sexe

- Lieu de naissance : code postal et commune pour un ressortissant français, ou code PMSI du pays pour un étranger.

3.2.2 Traits étendus

- Nom d'usage (le plus souvent, il s'agit du nom marital)
- Prénom d'usage (officiel ou habituellement utilisé par l'utilisateur)
- Autres prénoms de naissance
- Identifiant patient permanent (IPP)
- Numéro d'inscription au registre INSEE (NIR) personnel, destiné à devenir l'*identifiant national de santé* (INS).

3.2.3 Traits complémentaires

- Adresse de résidence de l'utilisateur ou de l'assuré
- Numéros de téléphone (portable et fixe)
- Adresse courriel de contact
- Nom des personnes en relation (parents, enfant, conjoint, personne de confiance...)
- Nom et coordonnées du médecin traitant
- Autres professionnels de santé impliqués dans la prise en charge
- Profession
- Document d'identité présenté
- Autres données de santé éventuellement utiles lors du traitement de doublons potentiels (ex : groupe sanguin).

3.3 Domaines d'identification et de rapprochement

Objet du chapitre : préciser les différents domaines d'identification et de rapprochement partageant des données de santé, au sein de la structure comme chez les partenaires connectés informatiquement.

Exemple de rédaction :

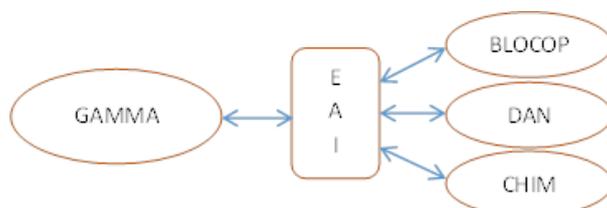
Plusieurs domaines d'identification coexistent au sein du système d'information hospitalier (SIH) de SSAN. Ils sont tous reliés au référentiel d'identité GAMMA qui est le serveur d'identités maître sur lequel se raccordent les principales applications utilisées dans l'établissement.

Le dossier patient informatisé (DPIX), qui est une application totalement dépendante de GAMMA en termes de gestion des identités, fait partie du même domaine d'identification que ce dernier.

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

- BLOCOP (gestion du bloc opératoire),
- DAN (dossier d'anesthésie),
- CHIM (circuit de chimiothérapie).

Ces domaines d'identification ont rapprochés de celui de GAMMA afin de garantir la cohérence des informations lors du parcours de chaque patient au sein de SSAN. Les identités sont transportées par une interface (EAI) qui permet de connecter les applications entre elles.



Les rapprochements avec les partenaires extérieurs au SSAN se font également au travers de l'interface EAI.

Toutes les applications gérant des identités patients font donc partie d'un même domaine de rapprochement (cf. 3.1.3). Les flux informatiques d'échanges entre les différents domaines répondent aux normes : HL7 ADT, HL7 PAM, HPRIM.

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

3.4 Confiance dans les identités gérées

Objet du chapitre : préciser les modalités mises en œuvre par la structure pour distinguer les identités provisoires de celles qui ont été validées avec un document d'identité.

Exemple de rédaction :

Conformément au référentiel régional de bonnes pratiques, SSAN met en œuvre des procédures permettant la gestion de l'état des identités.

Dans GAMMA, le référentiel d'identification de SSAN, il est possible d'attribuer à une identité 2 niveaux de confiance différents en fonction de la pièce justificative fournie par l'utilisateur :

- « Valide », qui correspond aux niveaux « certifié » ou « qualifié » du référentiel régional. Ce niveau est attribué automatiquement par l'application lors du renseignement du document d'identité présenté (liste définie par le COPILIV en accord avec le référentiel régional) ;
- « Provisoire », qui correspond au niveau de même nom du référentiel. C'est le niveau attribué par défaut lorsque le document d'identité présenté ne fait pas partie de la liste précédente.

GAMMA dispose également d'un champ « Douteux » qui peut être coché lorsque l'agent de l'accueil a un doute sur la validité d'un document présenté (patient étranger, difficultés de compréhension) ou suspecte une usurpation d'identité.

Les modalités pratiques de gestion de l'état d'identité sont précisées dans la procédure générale de recueil de l'identité, disponible dans la GED (cf. 4.1).

3.5 Identités particulières

Objet du chapitre : préciser les situations où la structure est amenée à gérer des identités sensibles (anonymat, confidentialité particulière...) et les organisations mises en œuvre pour les sécuriser.

Exemple de rédaction :

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

Elle est disponible dans la GED (cf. 4.1).

4 GESTION DES RISQUES A PRIORI

4.1 Gestion documentaire

Objet du chapitre : rappeler les modalités de gestion de l'ensemble de la documentation en lien avec l'identitovigilance.

Exemple de rédaction :

SSAN dispose d'un système de gestion électronique documentaire (GED) qui est géré par la CQGR pour la partie qui concerne les documents qualité. La CQGR est chargée de la diffusion de l'information sur la publication de nouveaux documents.

La GED intègre tous les documents relatifs à l'identitovigilance approuvés par la CLIV et validés par le COPILIV. Ils sont actualisés en tant que besoin et sont accessibles à l'ensemble des professionnels habilités à créer et gérer les identités patients (cf. 4.2).

Les documents en rapport avec l'identitovigilance comprennent :

- la présente charte d'identitovigilance ;
- les comptes rendus des instances (COPILIV, CLIV...);
- les protocoles, procédures et modes opératoires en vigueur dans la structure ;
- les documents régionaux mis à disposition par l'ARS.

4.2 Gestion des habilitations

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...).

Exemple de rédaction

Avant de pouvoir accéder au système d'information, tout nouvel arrivant doit préalablement signer la charte utilisateur du système d'information. Conformément à la politique de sécurité en vigueur, des droits d'accès lui sont attribués en fonction de son profil métier et de ses missions.

L'agent récupère son login et mot de passe auprès de la Direction des systèmes d'information (DSI). Ils lui sont remis contre émargement.

Toute sortie définitive de l'établissement est signalée à la DSI par la Direction des ressources humaines dans la semaine afin de supprimer les droits d'accès de la personne.

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

La direction des systèmes d'information tient à jour un certain nombre de documents qui sont actualisés en fonction des besoins :

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

4.3 Traçabilité des actions

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

Exemple de rédaction :

L'ensemble des applications informatiques liées aux données de santé utilisées par SSAN possèdent un dispositif d'enregistrement horodaté des accès précisant le nom (login), le type d'accès (lecture

ou écriture) et les pages visitées. En application de l'article R6113-9-2 du CSP la traçabilité des actions (création, modification et consultation) sont conservées pendant au moins 6 mois.

L'accès à ces informations n'est autorisé qu'à un nombre réduit de professionnels (directeur, DSI, responsable de la CLIV). Un contrôle peut être décidé lorsqu'il existe un doute sur le comportement d'un professionnel ou à titre systématique, par exemple pour vérifier l'absence d'intrusion externe dans le système d'information. Les modalités d'accès sont précisées dans une procédure *ad hoc* consultable sur la GED (cf. 4.1).

En termes d'identitovigilance, le système conserve pendant toute la durée de vie du dossier patient l'historique des modifications apportées sur les identités ainsi que des modifications apportées aux IPP (fusion de dossiers).

4.4 Information des usagers

Objet du chapitre : préciser les modalités d'information des usagers quant à la gestion de leurs données d'identité.

Exemple de rédaction :

Le livret d'accueil du patient de SSAN intègre un chapitre concernant la gestion de l'identité patient et les droits d'accès et de modification à ses données. Il précise l'importance d'une identification fiable et la nécessité de disposer de documents permettant de confirmer l'identité. Des informations sont également communiquées sur les écrans d'information mis en place aux admissions.

Pour l'ensemble des usagers, des documents (flyers, affiches) permettent également de les informer sur les règles d'identitovigilance et les pratiques de vérification de l'identité tout au long de sa prise en charge, notamment avant chaque acte de soins.

La conformité au RGPD fait également l'objet d'une information appropriée (cf. 2.5).

4.5 Formation et sensibilisation des acteurs

Objet du chapitre : préciser la politique mise en œuvre pour former et sensibiliser les acteurs sur le respect des règles d'identitovigilance (plan de formation interne, communication externe...).

Exemple de rédaction :

La politique d'identitovigilance est présentée à tous les nouveaux arrivants lors des sessions d'accueil des nouveaux professionnels. Le « guide des bonnes pratiques en identitovigilance » leur est remis à cette occasion.

Le plan de formation continue intègre des formations en lien avec l'identitovigilance. Cette formation est obligatoire dans les 6 mois suivant le recrutement d'un professionnel.

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

5 GESTION DES RISQUES A POSTERIORI

5.1 Gestion documentaire

Objet du chapitre : rappeler les modalités de gestion de la documentation relative à la déclaration et au suivi des événements indésirables liés à l'identitovigilance.

Exemple de rédaction :

On retrouve dans la GED (cf. 4.1) les documents relatifs à la gestion des risques *a posteriori*, c'est-à-dire aux actions à mettre en œuvre après la mise en évidence d'un dysfonctionnement relatif à

l'identification d'un patient : déclaration des événements indésirables, réalisation des enquêtes et des retours d'expérience adaptés aux erreurs d'identitovigilance...

5.2 Déclaration et gestion des événements indésirables

Objet du chapitre : préciser le dispositif mis en œuvre pour gérer les signalements des événements indésirables en relation avec l'identitovigilance.

Exemple de rédaction :

SSAN met en œuvre un système de signalement des événements indésirables (SSEI), piloté par la CGDR. Il promeut son emploi par l'ensemble des professionnels de l'établissement en priorisant les événements indésirables ayant un impact potentiel sur la sécurité des soins et notamment le signalement des erreurs en lien avec l'identification des patients.

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

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

Dès qu'une fiche d'événement indésirable (FEI) en lien avec l'identitovigilance est renseignée, celle-ci est transmise à la CGDR qui émet un accusé de réception et signale sa transmission à la CLIV pour traitement.

La CLIV est chargée, en relation avec les professionnels concernés, de réaliser le retour d'expérience (REX) et de mettre en œuvre des actions correctrices (cf. 5.3 et 5.4).

5.3 Gestion d'une erreur d'identité

Objet du chapitre : préciser l'organisation mise en œuvre pour assurer :

- la correction, au fil de l'eau, des erreurs d'identification signalées ;
- la transmission des informations aux autres domaines d'identités concernés ;

Exemple de rédaction :

Après signalement d'une erreur (cf. 5.2), la CLIV est chargée de mettre en œuvre les mesures correctrices adaptées à l'événement, en relation avec les professionnels concernés. Les délais de mise en œuvre de ces actions dépendent de la nature de l'évènement.

En cohérence avec le *référentiel régional*, la CLIV met à disposition dans la GED (cf. 4.1) des documents précisant :

- les modalités de traitement de certaines anomalies ou dysfonctionnements tels que la modification d'une erreur d'identité avérée, l'usurpation d'une identité... ;
- les professionnels habilités à réaliser ces actions, le contexte et la traçabilité des actions ;
- le mode de communication et de suivi interne des actions correctives à mettre en œuvre ;
- le système de diffusion du signalement intra et inter structures afin de transmettre aux autres domaines d'identification concernés (cf. 3.3) les informations relatives à une anomalie à corriger
- la conduite à tenir face à l'identification d'une erreur et les modalités d'information de la CLIV lorsqu'un événement indésirable est associé à une mauvaise gestion de l'identité.

Ces informations enrichissent une base de données tenue par la CLIV. Elle sert à la formation et à la sensibilisation des professionnels et à la mise à jour régulière des indicateurs de suivi (cf. 5.5).

5.4 Gestion des anomalies du domaine de rapprochement

Objet du chapitre : préciser l'organisation mise en œuvre pour assurer :

- analyse régulière de la base d'identités du domaine d'identification ;
- correction des erreurs (doublons...) ;
- transmission des informations aux autres domaines d'identités concernés ;

Exemple de rédaction :

La CLIV est chargée de s'assurer régulièrement de la qualité de la base de données des identités de chaque domaine d'identification mis en œuvre par SSAN.

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

- identification et gestion des doublons ;
- identification et gestion des collisions ;
- transmission des informations relatives à ces corrections aux autres domaines d'identité et professionnels concernés.

5.5 Indicateurs de suivi

Objet du chapitre : préciser les principaux indicateurs retenus par la structure pour évaluer le respect des règles d'identitovigilance et suivre les dysfonctionnements constatés (modalités de calcul, périodicité du recueil, devenir...).

Exemple de rédaction :

La CLIV suit un certain nombre d'indicateurs dans le domaine de l'identitovigilance qui ont pour objet de caractériser et de quantifier les problèmes de sécurité en lien avec l'identité des patients. Ils sont analysés à chaque réunion de la CLIV et font l'objet, si nécessaire, de propositions d'actions d'amélioration (cf. 2.3). Les actions retenues sont enregistrées, priorisées en fonction de leur niveau de criticité et font l'objet d'une évaluation afin de vérifier l'efficacité de leur mise en œuvre.

Principaux indicateurs suivis par la CLIV (à titre indicatif) :

- Nombre de signalements reçus en lien avec l'identitovigilance ;
- Taux de doublons détectés ;
- Taux de modifications d'identités réalisées après signalement d'anomalie ;
- Proportions d'identités certifiées et provisoires ;
- Taux de formation des professionnels à l'identitovigilance (par catégorie de professionnels) ;
- Part des erreurs liées aux différentes applications informatiques...

6 CONNEXION AU SERVEUR REGIONAL DE RAPPROCHEMENT

Objet du chapitre : préciser les conditions d'emploi et de sécurisation des données liées à l'utilisation du serveur de rapprochement d'identités (SRI) régional (si applicable).

Exemple de rédaction :

SSAN a signé en 2019 une convention d'engagement mutuel avec l'ARS NA pour l'utilisation du serveur de rapprochement d'identités (SRI) régional. La connexion est assurée par l'intermédiaire du référentiel d'identité (GAMMA) qui ne communique au SRI que les identités « Valides » (cf. 3.4).

Dans le cadre de cette connexion, SSAN est représenté par :

- un *référent identitovigilance*, interlocuteur privilégié auprès des instances régionales (CRIV, COTRIV), habilité à valider les rapprochements suggérés par l'interface de « gestion déléguée » du SRI ;
- un *référent technique* qui s'assure de la qualité des flux entre SSAN et le SRI et qui est en charge de la gestion des utilisateurs autorisés à accéder à l'interface de « gestion déléguée » du SRI.

Ces référents sont nommés par la CLIV dont ils font partie intégrante ; ils peuvent avoir un ou plusieurs suppléants.

Ils transmettent à la CLIV les indicateurs liés au fonctionnement du SRI en rapport avec les identités transmises par la structure. Pour exemples :

- nombre de rapprochements automatiques ou manuels ;
- nombre de modifications d'identités réalisées dans le cadre des rapprochements suggérés ;
- nombre de doublons potentiels et corrigés.

La communication aux usagers est assurée par l'intermédiaire de plusieurs vecteurs (cf. 2.5 et 4.4).

7 REFERENCES REGLEMENTAIRES ET TECHNIQUES

- Référentiel de bonne pratique en matière d'identitovigilance en région Nouvelle-Aquitaine (COTRIV, version du 11 décembre 2018)
- Instruction N° DGOS/MSIOS/2013/281 du 7 juin 2013 relative à l'utilisation du nom de famille (ou nom de naissance) pour l'identification des patients dans les systèmes d'information des structures de soins.
- Guide méthodologique de mise en œuvre de l'identité patient au sein des groupements hospitaliers de territoire (ASIP Santé, 2018)
- Convention d'engagement SRI.