IDENTITÉ NUMÉRIQUE
IDENTITOVIGILANCE
NOUVELLE-AQUITAINE

Comité technique régional d'identitovigilance de Nouvelle-Aquitaine

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

Version 2 – décembre 2020

Liste des contributeurs

Dr Bérénice BRECHAT-HUET, CH Cadillac

Mme Céline DESCAMPS, CRIV

Mme Johanna IZOTTE, ESEA

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, CRIV

Note de version

La version 1 de ce document, publiée en mai 2019, s'appuyait sur les exigences du *Référentiel régional de bonnes pratiques d'identitovigilance en Nouvelle-Aquitaine*.

La version 2 intègre les modifications nécessaires au respect des bonnes pratiques décrites dans le *Référentiel national d'identitovigilance* (RNIV) – qui remplace le référentiel régional - en les intégrant dans le plan initialement proposé.

Les parties modifiées par rapport à la version 1 sont surlignées en bleu.

PRÉAMBULE

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 les bonnes pratiques décrites dans le R*éférentiel national d'identitovigilance* (RNIV), le *Comité technique régional d'identitovigilance* (COTRIV) de Nouvelle-Aquitaine met à disposition des structures de santé un document type qui rappelle les éléments à retrouver de façon obligatoire dans la charte locale. Ce modèle de charte d'identitovigilance 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 référentiel 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 au plus près 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*.

STRUCTURE GÉNÉRALE

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. Éléments d'identification
   31. Terminologie
   32. Traits d'identification
   33. Domaines d'identification et de rapprochement
   34. Confiance dans les identités gérées
   35. Identités particulières
   36. Gestion de l'identité INS
4. Gestion des risques *a priori*
   41. Gestion documentaire
   42. Gestion des habilitations
   43. Gestion des accès « bris de glace »
   44. Traçabilité des actions
   45. Information des usagers
   46. 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 aux applications d'e-santé régionales (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 » pour bien identifier les usagers pris en charge afin de garantir leur sécurité tout au long de leur parcours. Elle définit l'organisation et les moyens mis en œuvre ainsi que les règles à respecter par l'ensemble des professionnels de l'établissement. Elle traite également des droits et devoirs des usagers qui sont également pleinement parties prenantes de leur propre sécurité.

2 POLITIQUE D'IDENTITOVIGILANCE

2.1 Définition et objectif

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

2.2 Engagement de la structure

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

Exemple de rédaction :

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 conforme aux préconisations du Référentiel national d'identitovigilance (RNIV). Les objectifs poursuivis sont de :

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

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

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 ;
- le référent en identitovigilance ;
- la cellule locale d'identitovigilance ;
- 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, en conformité avec les principes établis par le RNIV. Il s'assure de la mise à jour et de la cohérence des différentes applications du système d'information, valide les documents publiés par la structure dans ce domaine. Il se tient informé des résultats obtenus et des difficultés rencontrées. Il contrôle la cohérence du plan de formation avec les objectifs de formation et de sensibilisation des différents acteurs concernés.

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 référent en identitovigilance 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.

2.3.2 Le référent en identitovigilance

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

Exemple de rédaction :

Le responsable de la cellule d'identitovigilance est désigné comme *référent en identitovigilance* pour « SSAN ». Il est chargé, à ce titre, de :

- contribuer aux travaux de convergence du groupement d'établissements auquel appartient « SSAN » en matière d'identitovigilance ;
- représenter la « CLIV » aux réunions du « COPILIV » (cf. 2.3.1) et de l'instance de coordination des vigilances et des risques ;
- assurer la veille réglementaire et technique ;
- aider au repérage et à la gestion des risques liés à l'identification des usagers, en lien avec les autres vigilances et la cellule QGDR ;
- veiller à la promotion des bonnes pratiques dans son domaine, notamment par le biais de formations internes aux nouveaux arrivants et par la formation continue de l'ensemble professionnels ;
- informer sans délai le « COPILIV » des difficultés rencontrées en matière d'identitovigilance susceptibles de nuire à la sécurité des usagers ;
- participer à l'animation régionale par le biais de son adhésion au *réseau régional des référents en identitovigilance*.

2.3.3 La cellule 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 de « SSAN ». Elle a pour missions de participer, en lien avec la cellule QGDR, aux actions suivantes :

- sensibiliser l'ensemble des parties prenantes (professionnels, usagers) ;
- participer à la formation initiale et continue des professionnels amenés à créer ou modifier les identités dans le système d'information ;
- rédiger et/ou actualiser les procédures d'identitovigilance ;
- recueillir et analyser les évènements indésirables en lien avec l'identitovigilance ;
- contrôler la qualité des bases de données utilisées par la structure ;
- recueillir et analyser les indicateurs qualité ;
- mettre en place les actions préventives et/ou correctives souhaitables.

La « CLIV » comprend les personnes référentes suivantes :

- le responsable de la CLIV, assurant la fonction de référent local en identitovigilance (cf. 2.3.2) ;
- 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 ;
- un cadre de santé ;
- des correspondants d'identitovigilance ;
- des référents logiciels ;
- un représentant d'usager.

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, sous l'autorité du référent en identitovigilance, 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 ».

2.3.4 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).

Exemple de rédaction :

- **Correspondants en identitovigilance internes**

  Chaque service clinique et médicotechnique de « SSAN » désigne au moins un correspondant en 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 en identitovigilance est affichée dans chaque service.

- **Correspondants en identitovigilance externes**

  Les structures partenaires (cabinet de radiologie « RADIOSARL » et laboratoire de biologie « MEDILAB ») sont invitées à identifier des correspondants en identitovigilance et à transmettre leurs coordonnées à la « CLIV » de « SSAN ». Ils ont pour objet de faciliter la mise en commun des règles d'identitovigilance mais aussi de participer au signalement et au traitement des erreurs dans le cadre des données de santé échangées (domaine de rapprochement, cf. 3.3).

  Ces correspondants sont invités à participer aux réunions et actions de la « CLIV » pour les sujets qui les concernent.

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

2.3.5 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'usagers, chaque application est pilotée par un *référent logiciel*.

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 avec le référentiel d'identités « GAMMA » de « SSAN », 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).

Les différents référents logiciels s'assurent de la qualité des flux de transmission des données d'identification et de leur bonne intégration dans les services clients. Ce contrôle fait intervenir, si beoin, les référents en identitovigilance concernés.

La « CLIV » dispose de la liste de l'ensemble des référents logiciels et des applications qu'ils gèrent. 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 (ou, si applicable, du groupement de structures).

Exemple de rédaction :

La politique d'identitovigilance concerne l'ensemble des applications gérées par « SSAN » qui permettent d'identifier les usagers au travers du référentiel d'identités « GAMMA ». Le « COPILIV » s'assure que les autres domaines d'identification échangeant des données avec les applications de la structure (cf. 2.3.4 et 3.3) disposent également d'une politique d'identitovigilance compatible avec celle de SSAN et de protocoles d'interopérabilité *ad hoc*.

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 l'utilisation des services régionaux (cf. 6).

Un document d'information sur l'utilisation de ces services est affiché dans les lieux d'accueil administratifs et dans le livret d'accueil de l'établissement (cf. 4.5). 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.

3 ÉLÉMENTS 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 consiste à recueillir les informations (traits) représentant une personne physique pour l'identifier de façon unique. Ces traits d'identification sont utilisés comme critères pour rechercher le patient dans le système d'information. Ils concourent à la sécurité de sa prise en charge.

3.1.2 Identité et identifiant numériques

Identité numérique : représentation de l'identité d'une personne physique dans un système d'information. L'identité numérique est composée d'un ou plusieurs identifiant(s) numérique(s) et de traits d'identification (cf. 3.1.4).

Identifiant numérique : 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.

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

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

- *l'identifiant d'épisode patient* (IEP) qui est créé pour chaque événement relatif au séjour du patient : c'est le numéro de séjour ;
- *l'identifiant permanent patient* (IPP) qui est créé pour chaque nouveau patient non encore connu de l'établissement. Chaque patient a donc un IPP unique[1], constant dans le temps, auquel sont raccrochés les identifiants de venue ;
- le matricule INS qui correspond au numéro d'inscription au registre de l'INSEE (NIR ou NIA) associé à l'identité INS.

3.1.3 Domaine d'identification et de rapprochement

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

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

NB : le rapprochement entre 2 identités numériques est également possible au sein d'un même DI ; il correspond à la recherche et au traitement des doublons; on parle alors de « fusion » des identités numériques en doublon en une seule (cf. 3.1.5).

3.1.4 Traits d'identification

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

En cohérence avec le RNIV, « SSAN » distingue 2 catégories de traits d'identification (cf. 3.2).

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

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

3.1.5 Doublons, fusion, collisions

Les termes employés en identitovigilance sont définis dans l'annexe II du volet socle du RNIV (*1. Principes d'identification des usagers communs à tous les acteurs de santé*). Il n'en sera précisé que certains dans cette charte qui ont une importance toute particulière en termes de qualité et de sécurité de la prise en charge.

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

3.2 Traits d'identification

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 opposables.

Exemple de rédaction :

Conformément au RNIV, « SSAN » classe les traits d'identification qu'il utilise selon 2 catégories (cf. 3.1.4). Une procédure interne définit comment sont retenus et vérifiés ces différents traits.

3.2.1 Traits stricts

- *Nom de naissance* ;
- *Premier prénom* d'état civil ;
- *Liste des prénoms* de naissance figurant sur un titre officiel d'identité ;
- *Date de naissance* ;
- *Sexe* ;
- *Lieu de naissance*, sous forme de code INSEE de la commune (pour les usagers nés en France) ou du pays (pour les autres) ;
- *Matricule INS* (toujours associé à son OID[2]).

3.2.2 Traits complémentaires

- *Nom utilisé* (le « COPILIV » a fait le choix de rendre obligatoire l'enregistrement de cette donnée relative au nom utilisé par l'usager dans la vie courante, qu'il s'agisse du nom de naissance, du

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

nom d'usage lié à un acte d'état civil ou de tout autre nom (pseudonyme) utilisé de façon notoire) ;
- *Prénom utilisé* (le « COPILIV » a fait le choix de rendre obligatoire l'enregistrement de cette donnée, qu'il s'agisse du premier prénom de l'état civil ou de tout autre prénom utilisé par l'usager dans la vie courante) ;
- *Code postal* de la commune de naissance (pour les usagers nés en France exclusivement) ;
- *Commune de naissance* (donnée à renseigner de façon obligatoire pour un ressortissant français et chaque fois que possible pour un étranger) ;
- *Identifiant patient permanent* (IPP) ;
- *Adresse de résidence* de l'usager ou de l'assuré ;
- Numéros de téléphone (portable et fixe) ;
- Adresse(s) courriel de contact ;
- Nom des personnes en relation (parents, enfant, conjoint, personne de confiance…) ;
- Nom et coordonnées de la personne de confiance ;
- Nom et coordonnées du médecin traitant ;
- Autres professionnels de santé impliqués dans la prise en charge ;
- Profession ;
- Type de document d'identité présenté.

3.3 Domaines d'identification et de rapprochement

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.

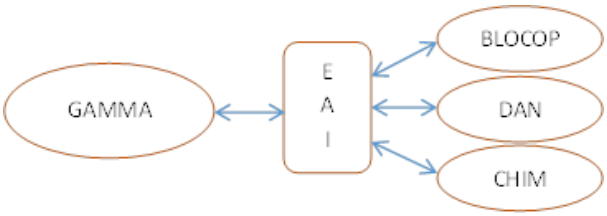
Exemple de rédaction :

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 référentiel d'identités numériques 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 numériques, fait partie du même domaine d'identification que ce dernier.

D'autres logiciels, qui utilisent une base de données d'identités numériques 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 sont « rapprochés » de celui de « GAMMA » afin de garantir la cohérence des informations lors du parcours de chaque patient au sein de « SSAN ». Les identités numériques sont échangées par le biais d'une interface (EAI) qui permet de connecter les applications entre elles.



Les rapprochements avec les partenaires extérieurs au « SSAN » se font également au travers d'une interface EAI.

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

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 différents niveaux de confiance associées aux identités numériques en fonction des modalités de récupération ou de contrôle.

Exemple de rédaction :

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

Dans « GAMMA », le référentiel d'identités de « SSAN », chaque identité numérique est associée à un des 4 statuts de confiance suivants :
- « Identité provisoire » ;
- « Identité validée » ;
- « Identité récupérée » ;
- « Identité qualifiée ».

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

3.5 Identités particulières

Objet du chapitre : préciser les situations où la structure est amenée à gérer des identités particulières et les organisations mises en œuvre pour les sécuriser.

Exemple de rédaction :

« GAMMA » met à disposition des professionnels 3 attributs facultatifs qui permettent de caractériser certaines situations spécifiques :
- « Identité douteuse » pour signaler un doute sur la véracité d'un document présenté (difficultés de compréhension d'un patient étranger, suspicion d'utilisation frauduleuse d'identité…) :
- « Identité fictive », utilisé pour caractériser la création d'une identité numérique ne reposant pas sur les traits réels de l'usager pris en charge (anonymat, identités sensibles) ;
- « Identité homonyme » qui permet d'alerter l'ensemble des utilisateurs d'une identité numérique qu'il existe d'autres usagers dans le référentiel d'identités de « SSAN » dont les traits d'identité sont approchants, donc à fort risque d'erreur.

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

La gestion des identités douteuses et des identités approchantes fait également l'objet de procédures spécifiques.

Elles sont disponibles dans la GED (cf. 4.1).

3.6 Gestion de l'identité INS

Objet du chapitre : préciser les modalités de récupération et de vérification de l'identité INS.

Exemple de rédaction :

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

Des procédures *ad hoc* précisent les conditions dans lesquelles le téléservice INSi est appelé et la gestion des identités numériques qui en découle, soit en mode « recherche et récupération », soit en mode « vérification d'une identité INS ». Elles sont disponibles 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 qui prennent en charge l'usager, dans leur domaine de compétence (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 de portée régionale et nationale mis à disposition par les instances régionales d'identitovigilance.

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 plus ou moins étendus lui sont attribués en fonction de son profil métier et de ses missions, tels qu'ils sont décrits dans la matrice des droits.

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 (DRH) 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 liste des professionnels et des droits attribués.

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 Gestion des accès « bris de glace »

Objet du chapitre : préciser les modalités d'accès aux informations protégées en cas d'urgence par des professionnels non habilités.

Exemple de rédaction :

L'accès au dossier patient informatique d'un usager par un professionnel qui n'en a pas les droits (remplaçant, nouvel arrivant…) peut exceptionnellement être autorisé en situation d'urgence afin qu'il puisse prendre connaissance des données de santé nécessaire à sa prise en charge. Cette modalité d'accès dite « bris de glace » est décrite dans une procédure *ad hoc* consultable sur la GED (cf. 4.1).

4.4 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 code de la santé publique, la traçabilité des actions (création, modification et consultation) sont conservées pendant au moins 6 mois.

L'accès à ces informations n'est autorisé qu'à un nombre réduit de professionnels (directeur, DSI, responsable de la 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 numériques, y compris les modifications apportées aux IPP (fusion de dossiers).

4.5 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).

4.6 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 évènements 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).

Lorsque les conséquences sont graves, le signalement des événements indésirables est réalisée selon les consignes applicables, soit par le biais du portail national de signalement des événements sanitaires indésirables – lorsque l'EI est éligible – soit directement à l'ARS.

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 RNIV, 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, la suspicion d'utilisation frauduleuse 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 ainsi qu'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 l'instance 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 UTILISATION DE SERVICES D'E-SANTÉ RÉGIONAUX

Objet du chapitre : préciser les conditions d'emploi et de sécurisation des données liées à l'utilisation des applications d'e-santé régionales. Si l'établissement n'est pas concerné, le chapitre doit être conservé mais indiqué comme « Non applicable ».

Exemple de rédaction :

« SSAN » utilise certains services d'échange et de partage de données de santé mis à disposition au niveau régional pour améliorer les parcours de santé.

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

Afin de garantir le respect des termes de la convention, « SSAN » confie à chaque référent logiciel concerné par l'utilisation d'un service la mission de s'assurer de la conformité des échanges de données numériques entre le logiciel et l'application régionale utilisée par rapport aux exigences techniques et réglementaires applicables. Il est notamment en charge de la mise en œuvre effective d'une procédure d'alerte réciproque entre « SSAN » et :
- le porteur de la solution en cas d'événement indésirable relatif aux problèmes d'interopérabilité ;
- la cellule régionale d'identitovigilance (CRIV) si l'événement indésirable est associé à l'identification de l'usager ou à la diffusion erronée d'une identité INS incorrecte.

Des procédures *ad hoc* sont formalisées, en lien avec le référent local en identitovigilance, et consultables dans la GED (cf. 4.1).

Les erreurs d'identification peuvent également justifier un signalement externe (cf. 5.2).

La communication de l'utilisation de ces services aux usagers est assurée par l'intermédiaire de plusieurs vecteurs (cf. 2.5 et 4.5).

7 RÉFÉRENCES RÉGLEMENTAIRES ET TECHNIQUES

- Référentiel national d'identitovigilance (RNIV)
- Instruction….
- Guide méthodologique de mise en œuvre de l'identité patient au sein des groupements hospitaliers de territoire (ASIP Santé, 2018)
- Modèle régional de charte d'identitovigilance des établissements sanitaires et médico-sociaux (V2)