****

MODÈLE RÉGIONAL
DE CHARTE D’IDENTITOVIGILANCE

**a l’attention DES ÉTABLISSEMENTS
DE SANTE**

Version 1 – Septembre 2021

La version 1 de ce document s’appuie sur le *Référentiel national d’identitovigilance* (RNIV).

Ce document a été produit en s’appuyant sur les travaux réalisés par « e-santé en action » (ESEA) Nouvelle Aquitaine dans le cadre de la collaboration inter-régionale à travers le Réseau des Référents Régionaux d’IdentitoVigilance (3RIV).

Il a été validé par l’instance régionale de pilotage de l’identitovigilance de Bretagne.

# Préambule

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

Elle est utilisée pour définir des engagements pris par les signataires vis-à-vis des usagers (charte de la personne hospitalisée, charte des résidents, 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 établissement 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…



Figure 1 : Contenu de la charte identitovigilance tel que prévu par le RNIV 2

Afin d’harmoniser les différentes chartes existantes et de s’assurer de leur conformité avec les bonnes pratiques décrites dans le *Référentiel national d’identitovigilance* (RNIV), le GCS e-Santé Bretagne et la SRA CAPPS Bretagne mettent à disposition des établissements un document type qui rappelle les éléments à retrouver en son sein. Ce modèle de charte d’identitovigilance est à adapter par chaque établissement en fonction de ses spécificités organisationnelles et techniques.

# Mode d’emploi

Le présent document constitue un modèle de charte d’identitovigilance que l'instance régionale de pilotage de l’identitovigilance préconise d’utiliser en Bretagne. 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.

Pour formaliser la charte d’identitovigilance de leur établissement, 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 ;
* supprimer, à la fin du processus, les chapitres « Préambule » et « Mode d’emploi ».

Des recommandations opérationnelles ne figurant pas dans le RNIV sont proposées dans ce modèle de charte : elles sont surlignées en jaune dans le présent document.

# Structure générale

La structure générale d’une charte d’identitovigilance, illustrée dans les chapitres du présent document, est la suivante (sans parler de la page de garde avec le nom de l’établissement, 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 l’établissement

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. Liste des points de création d’identités de l’établissement

35. Cartographie applicative de l’établissement

36. Confiance dans les identités gérées

37. Identités particulières

38. Gestion de l’identité INS

39. Identification secondaire

4. Gestion des risques

41. Gestion des risques *a priori*

42. Gestion des risques *a posteriori*

5. Références réglementaires et techniques

# 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 l’établissement 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 en tant qu’acteurs à part entière de la politique d’identitovigilance.

# Politique d’identitovigilance

## Définition et objectif

Objet du chapitre : définir l’identitovigilance et décrire les objectifs de l'établissement en termes de bonnes pratiques d’identification des 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 de l’usager afin d’éviter les risques d’erreurs tout au long de son parcours.

Les règles d’identitovigilance définies par le *Référentiel national d’identitovigilance* (RNIV) s’imposent à l’ensemble des acteurs 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 l'établissement ou lors des échanges avec les référents du parcours de l’usager, dans le respect du secret médical.

## Engagements de l'établissement

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

Exemple de rédaction :

La direction de l’établissement, 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 les suivants :

* 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 de l’usager ;
* sensibiliser les différents acteurs – internes et externes à l'établissement – impliqués dans ces démarches.

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

## Gouvernance

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

* de conduite de la politique d’identitovigilance dans l'établissement ;
* 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 l’établissement, repose sur une organisation spécifique qui comprend :

* une instance stratégique
* une instance opérationnelle
* une instance consultative : non obligatoire (sur décision de l’instance stratégique)
* un référent identitovigilance

Le rôle des référents logiciels est décrit dans le chapitre *2.3.5 Référents logiciels*. Acteur à part entière, et obligatoire de la politique d’identitovigilance, le référent logiciel n’est toutefois pas identifié par le RNIV comme un membre de la gouvernance en identitovigilance de l’établissement.

### L’instance stratégique

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

Exemple de rédaction :

L’instance stratégique a pour objet de définir les orientations de la politique d’identitovigilance, l’organisation et les moyens à mettre en œuvre pour la faire respecter, en conformité avec les principes établis par le RNIV.

Elle est notamment chargée :

* de participer à la définition de la politique d’identitovigilance et de formation des acteurs dans ce domaine ;
* d’arrêter l’organisation à mettre en œuvre (structuration des instances, missions qui leur sont confiées) ;
* de définir les moyens humains, techniques et financiers à attribuer pour le fonctionnement optimal de cette organisation ;
* de valider le plan annuel ou pluriannuel d’actions à conduire ;
* de suivre les actions et leurs résultats en s’appuyant sur des indicateurs pertinents ;
* de décider des actions correctives à mettre en œuvre ;
* de communiquer sur la politique et ses résultats.

Il est préconisé d’intégrer les actions d’amélioration validées au sein de l’instance stratégique au programme d’amélioration de la qualité et de la sécurité (PAQSS) de l’établissement.

La composition recommandée de l’instance stratégique 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 responsable de la sécurité des systèmes d’information (RSSI) ;
* le coordonnateur de la gestion des risques associés aux soins ;
* le délégué à la protection des données (DPO) rattaché à l’établissement ;
* le responsable des admissions.

Elle peut compter, en tant que membres associés :

* des représentants des domaines satellites (pharmacie, imagerie, laboratoire, bloc...) ;
* des référents en identitovigilance des structures partenaires ;
* des représentants des usagers. ;
* un représentant du service des archives ;
* le correspondant local en hémovigilance et sécurité transfusionnelle.

La composition de cette instance stratégique dépend de la taille et de l’activité de l’établissement.

Pour les établissements faisant partie d’un groupement hospitalier de territoire (GHT) ou d’un groupe d’établissements privés, l’instance stratégique peut être celle du niveau de décision le plus élevé.

La liste actualisée des membres de l’instance stratégique est disponible dans la gestion documentaire (GED, cf. 4.1.1).

L’instance stratégique se réunit au moins une fois par semestre.

Sa composition, ses objectifs et ses modalités de fonctionnement sont formalisés au sein d’un règlement intérieur. Chaque réunion donne lieu à la rédaction d’un compte rendu ou d’un relevé d’informations-décisions-actions.

### L’instance opérationnelle

Objet du chapitre : préciser les missions et la composition de la structure chargée de la conduite opérationnelle de l’identitovigilance dans l’établissement. L’instance opérationnelle est le plus souvent dénommée *cellule d’identitovigilance (CIV).*

Exemple de rédaction :

L’instance opérationnelle a pour missions de participer, en lien avec la cellule QGDR, aux actions suivantes (liste non exhaustive):

* participer à la formation des professionnels amenés à créer ou modifier les identités dans le système d’information, dans le cadre du plan de formation de l’établissement ;
* rédiger et/ou actualiser les documents relatifs à l’identitovigilance ;
* contrôler la qualité des identités dans les domaines d’identification utilisés par l'établissement ;
* définir, suivre et analyser les indicateurs relatifs à l’identitovigilance ;
* initier et mener des actions de sensibilisation des usagers et des partenaires externes ;
* réaliser une cartographie des risques comprenant notamment les risques liés à la sécurité informatique ;
* prendre part aux retours d’expériences des événements indésirables en lien avec les erreurs d’identification;
* réaliser des audits de connaissance et de pratiques ;
* guider les professionnels sur la conduite à tenir vis-à-vis des cas particuliers ;
* réaliser le traitement des anomalies signalées (doublons, collisions...) ;
* contribuer au rapprochement d’identités entre structures ;
* réaliser la veille réglementaire et technique.

Elle rend compte à l’instance stratégique des actions conduites et des difficultés rencontrées.

Les professionnels composant l’instance opérationnelle, identifiés pour leurs compétences en identitovigilance, sont désignés par le responsable de la structure et placés sous l’autorité technique du référent en identitovigilance. Il peut s’agir de personnels médicaux, paramédicaux, administratifs, médico-administratifs …

L’instance opérationnelle peut, par exemple, être composée :

* du responsable de l’instance opérationnelle, assurant la fonction de référent local en identitovigilance (cf. 2.3.2) ;
* du responsable de l’accueil et de la facturation ;
* d’un représentant de la DSI ;
* du responsable de la CQGR ;
* du coordonnateur de la gestion des risques associés aux soins ;
* d’un cadre de santé ;
* des correspondants d’identitovigilance ;
* des référents logiciels ;
* d’un représentant des usagers.

La liste actualisée des membres de l’instance opérationnelle est disponible dans la GED (cf. 4.1.1).

L’instance opérationnelle assure un fonctionnement quotidien au moins pendant les heures ouvrables. Sous l’autorité technique du référent en identitovigilance, elle 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 au sein de son rapport annuel transmis à l’instance stratégique

La composition, les objectifs et les modalités de fonctionnement de l’instance opérationnelle sont formalisés au sein d’un règlement intérieur. Chaque réunion donne lieu à la rédaction d’un compte-rendu ou d’un relevé d’informations-décisions-actions.

### 2.3.3 L’instance consultative

Il n’est pas obligatoire de mettre en place une instance consultative au niveau de la structure ; cela relève de la décision de l’instance stratégique correspondante. Si c’est le cas, elle doit être constituée de représentants des différentes catégories professionnelles impliquées dans les questions d’identification afin de donner un avis sur la politique, la formation ou les documents qualité qui leur sont soumis :

* membres de la CIV ;
* référents logiciels ;
* représentants des parties prenantes (professionnels de santé, médico-sociaux, usagers, développeurs informatiques, sous-traitants, responsables de systèmes d’information…).

Il peut être décidé de mettre en place une instance consultative au niveau du groupement hospitalier de territoire (GHT) ou du groupe d’établissements privés en faisant notamment appel à des représentants des différentes instances opérationnelles et/ou stratégiques des structures qui la composent.

### 2.3.4 Le référent en identitovigilance

Objet du chapitre : préciser les missions du référent en identitovigilance de l'établissement.

Exemple de rédaction :

Le référent en identitovigilance est membre de l’instance stratégique et de l’instance opérationnelle (placée sous son autorité technique). Il est nommé par la direction, en concertation avec le président de la commission médicale d’établissement, sur proposition de celle-ci. Il dispose d’une fiche de poste et d’un temps dédié.

Le référent en identitovigilance est chargé de :

* promouvoir les bonnes pratiques d’identitovigilance conformément aux exigences règlementaires et aux recommandations nationales et régionales applicables ;
* piloter la cellule opérationnelle afin qu’elle réponde aux besoins des parties prenantes ;
* Représenter la structure dans l’instance consultative régionale d’identitovigilance ;
* participer à la gestion des risques liés aux erreurs d’identification et à la coordination des vigilances ;
* alerter le responsable de l'établissement sur les difficultés rencontrées en matière de lutte contre les risques relatifs à l’identitovigilance.

Le référent en identitovigilance est identifié au niveau de l’établissement, et dans l’observatoire des systèmes d’information en santé (oSIS) de la plateforme ATIH (dès que cette inscription sera permise).

### Référents logiciels

Objet du chapitre : préciser le rôle des référents logiciels.

Exemple de rédaction :

Le système d’information de l’établissement 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*.

Acteur à part entière, et obligatoire de la politique d’identitovigilance, le référent logiciel n’est toutefois pas identifié par le RNIV comme un membre de la gouvernance en identitovigilance de l’établissement.

Il est le correspondant privilégié du référent en identitovigilance de la structure pour tout ce qui concerne l’identité de l’usager. 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.

La liste des applications informatiques partageant des données de santé nominatives, et donc intégrées au domaine d’identification de l’établissement, 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 besoin, les référents en identitovigilance concernés.

L’instance opérationnelle 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. 4.1.1).

## 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 l’établissement qui permettent d’identifier les usagers au travers de son référentiel d’identités. A ce titre, l’instance opérationnelle contrôle la qualité des identités dans les domaines d’identification utilisés par la structure, et contribue au rapprochement d’identités avec les domaines d’identification externes, échangeant des données avec les applications de l’établissement.

## Respect du RGPD

Objet du chapitre : préciser les modalités mises en œuvre par l'établissement 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 l’établissement a formalisé, sous l’autorité de son délégué à la protection des données (DPO), la documentation prévue par le *Règlement général de protection des données* (RGPD), y compris pour l’utilisation de ces données dans le cadre de l’utilisation des services régionaux.

Un document d’information sur l’utilisation de ces services est affiché dans les lieux d’accueil administratifs et dans le livret d’accueil de l’établissement (cf. 4.1.5). 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. Il comporte les mentions d’information relatives à la collecte et au traitement de l’INS.

# Éléments d’identification

## Terminologie

Objet du chapitre : préciser les définitions des termes employés dans les documents d’identitovigilance de l'établissement.

Exemple de rédaction :

L’objet de ce chapitre est de rappeler la signification des termes techniques utilisés dans l’établissement en matière d’identification des usagers.

### Identification

Identifier une personne consiste à disposer des informations nécessaires et suffisantes pour ne pas la confondre 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.

### Identité et identifiant numériques

**Identité numérique** : représentation d’un individu physique dans un système d’information.

**Identifiant (technique)** : séquence de caractères alphanumériques utilisée par un ou plusieurs systèmes d’information pour représenter une personne physique. Par exemple : identifiant permanent du patient (IPP), matricule INS…

**Identité nationale de santé (INS)**: c’est une identité numérique unique, univoque, pérenne, permettant de référencer, de conserver et de transmettre les informations de santé d’un usager. Son utilisation est obligatoire à compter du 01/01/2021 par l’ensemble des professionnels de santé. Elle correspond aujourd’hui à l’identité INS.

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

* *l’identifiant d’épisode patient* (IEP) qui est créé pour chaque événement relatif au séjour du patient : c’est le numéro de séjour ;
* *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]](#footnote-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.

### Domaine d’identification et de rapprochement

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.

Le rapprochement d’identités est l’opération qui consiste à attribuer une identité numérique (dite identité de fédération) commune à plusieurs identités numériques appartenant à des domaines d’identification différents (au niveau territorial, régional) mais qui font référence au même usager.

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 (cf. 3.1.5).

### 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, prénom, date de naissance, sexe.

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

* Les **traits stricts** : ce sont les informations de référence qui caractérisent l’identité sanitaire officielle de l’usager ; elles permettent de référencer les données de santé partagées et de fiabiliser les rapprochements d’identités numériques entre structures.
* Les **traits complémentaires** : ce sont des données qui apportent d’autres informations utiles à la prise en charge de l’usager. Par exemple adresse, nom et/ou prénom utilisé…

### 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**: on parle de doublons d’identités lorsqu’une même personne est enregistrée sous 2 identifiants différents (ou plus) dans un même domaine d’identification. On dispose alors pour l’usager de plusieurs dossiers médicaux et administratifs différents qui ne communiquent pas entre eux. Le fait de ne pas disposer de l’ensemble des informations médicales concernant l’usager engendre un risque lié à la méconnaissance, par le professionnel, de données utiles à la prise de décision.
* La **fusion** correspond au transfert, sur un identifiant unique, de toutes les informations concernant le même usager dispersées sur plusieurs identifiants (doublons) d’un même domaine d’identification.
* La **collision** est une anomalie correspondant à l’attribution d’un même identifiant à 2 personnes physiques différentes, ou plus, notamment dans les cas suivants : sélection erronée d’un dossier informatique, usurpation d’identité d’un tiers déjà enregistré, erreur d’opération de fusion entre dossiers n’appartenant pas au même usager… Il devient très difficile dans ce cas de faire la part, a posteriori, des informations médicales qui relèvent de chaque usager. Le risque est de prendre des décisions médicales et soignantes au regard des données de santé d’une autre personne.

## Traits d’identification

Objet du chapitre : préciser les traits d’identification et les règles d’enregistrement retenus au sein de l’établissement et leur cohérence avec les règles d’identitovigilance opposables.

Exemple de rédaction :

Conformément au RNIV, l’établissement 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.

### Traits stricts

* *Nom de naissance*;
* *Premier prénom* de naissance ;
* *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 patients nés en France) ou du pays (pour les patients nés à l’étranger) ;
* *Matricule INS* (toujours associé à son OID[[2]](#footnote-2)).

### Traits complémentaires

* *Nom utilisé* : à la place du nom d’usage, qui a une définition légale, le RNIV crée le terme de nom utilisé pour permettre l’enregistrement du nom réellement porté dans la vie courante, qu’il s’agisse du nom de naissance ou du nom d’usage, voire, sous certaines conditions, celui utilisé dans le pseudonyme ou le surnom de l’usager. Ce trait complémentaire a pour objet de faciliter le dialogue soignant-soigné.
* *Prénom utilisé* : à la place du prénom usuel, qui a une définition légale, le RNIV crée le terme de prénom utilisé pour permettre l’enregistrement du prénom réellement porté dans la vie courante. Il peut s’agir d’un des prénoms de naissance, du prénom d’usage voire, sous certaines conditions, d’un autre prénom non officialisé – comme cela peut être habituel dans certaines régions – ou utilisé dans le pseudonyme ou le surnom de l’usager. Ce trait complémentaire a pour objet de faciliter le dialogue soignant-soigné.
* *Code postal* et/ou *nom de la commune de naissance*
* *Adresse postale* de l’usager;
* *Numéros de téléphone* de l’usager ou de son tuteur ;
* *Adresse mail* de l’usager ou de son tuteur ;
* *Photographie* (sous réserve du respect du droit à l’image et des règles de conservation des données en vigueur) ;
* *Numéro de sécurité sociale* de l’ouvrant droit (il concerne les différents ayants droit d’un seul assuré) ;
* *Identités et coordonnées des personnes en relation* (parents, enfant, conjoint, personne de confiance…) ;
* *Coordonnées du médecin traitant* ;
* *Autres professionnels de santé impliqués dans la prise en charge* ;
* *Profession* ;
* *Nature du document d’identité présenté* ;
* Etc.

## 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 l’établissement comme chez les partenaires connectés informatiquement.

Exemple de rédaction :

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

Le dossier patient informatisé (« DPI»), qui est une application totalement dépendante du référentiel d’identités 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 du référentiel d’identités (sur le schéma : “GAMMA”) afin de garantir la cohérence des informations lors du parcours de chaque usager. 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 de l’établissement 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 le référentiel d’identités de l’établissement que sont gérés les numéros de séjour (IEP) et les mouvements du patient.

## Liste des points de création d’identités de l'établissement

Objet du chapitre : l’établissement insère ici la liste des points de création d’identités présents en son sein.

## Cartographie applicative de l'établissement

Objet du chapitre : afin d’identifier les modalités de mise en conformité INS, l’établissement insère ici un lien vers sa cartographie applicative qui permet de lister et catégoriser les logiciels.

## Confiance dans les identités gérées

Objet du chapitre : préciser les modalités mises en œuvre par l'établissement pour distinguer les différents niveaux de confiance associés aux identités numériques en fonction des modalités de récupération ou de contrôle.

Exemple de rédaction :

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

Dans son référentiel d’identités, 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. 4.1.1).

## Identités particulières

Objet du chapitre : préciser les situations où l'établissement est amené à gérer des identités particulières et les organisations mises en œuvre pour les sécuriser.

Exemple de rédaction :

Le référentiel d’identités met à disposition des professionnels 3 attributs facultatifs qui permettent de caractériser certaines situations spécifiques :

* « Identité douteuse » : attribut d’une identité numérique utilisé pour signaler que la procédure d’identification n’est pas sûre, soit du fait d’un doute sur le document d’identification présenté (suspicion de fraude), soit parce que l’identité est relevée sur les dires d’un patient confus ou d’un tiers qui le connaît mal. C’est un attribut qui ne peut être associé qu’au statut d’identité provisoire.
* « Identité fictive » : attribut d’une identité numérique utilisé pour signaler que les traits d’identité n’ont pas de rapport avec l’identité réelle de l’usager. Il découle de la mise en œuvre d’une procédure d’identification applicable aux situations d’identités sensibles (anonymisation de la prise en charge). Cet attribut peut également servir dans le cadre de tests informatiques ou de formations. C’est un attribut qui ne peut être associé qu’au statut d’identité provisoire.
* « Identité homonyme » : attribut utilisé pour signaler un fort taux de ressemblance entre des identités numériques et alerter les professionnels lors de la prise en charge de ces usagers homonymes ou à identités approchantes.

L’établissement assure la confidentialité relative aux prises en charge effectuées en son sein. 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. 4.1.1).

## 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, l’établissement 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. 4.1.1).

## Identification secondaire

Objet du chapitre : l’établissement détaille ici les procédures d’identification secondaire mises en place en son sein.

Exemple de rédaction :

Les bonnes pratiques d’identification primaire ne permettent pas, à elles seules, de sécuriser la prise en charge des usagers. Afin de s’assurer que l’usager bénéficiaire de l’acte est bien celui pour lequel le soin a été prescrit, l’établissement a mis en place les procédures suivantes :

[…]

# Gestion des risques

La gestion des risques liée aux erreurs d’identification est l’une des missions prioritaires des instances en charge de l’identitovigilance. Elle doit être conduite **en association étroite avec les professionnels dédiés à la gestion des risques de la structure** : direction ou service qualité gestion des risques (CQGR), coordonnateur de la gestion des risques associés aux soins, responsable du système de management de la qualité de la prise en charge médicamenteuse, référent local en identitovigilance, référents des différentes vigilances réglementaires, responsable des systèmes d’information …

## Gestion des risques *a priori*

### Gestion documentaire

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

Exemple de rédaction :

A minima, le RNIV prévoit que l’ensemble des documents relatifs à la sécurisation de l’identification ont vocation à être réunis dans un manuel qualité dédié à l’identitovigilance (proposé sous forme GED dans le présent modèle).

L’établissement dispose d’un système de gestion électronique documentaire (GED) qui est géré par la CQGR pour la partie qui concerne les documents qualité. La Cellule d’identitovigilance est chargée de formaliser et/ou d’actualiser les documents qualité relatifs à l’identitovigilance. La CQGR est chargée, quant à elle, de la diffusion de l’information sur la publication de nouveaux documents. La GED intègre tous les documents relatifs à l’identitovigilance. Ils sont actualisés en tant que besoin et sont accessibles à l’ensemble des professionnels qui prennent en charge l’usager, dans leur domaine de compétence.

Les documents en rapport avec l’identitovigilance comprennent notamment :

* la présente charte d’identitovigilance ;
* les comptes rendus des instances (instance stratégique, instance opérationnelle…) ;
* les protocoles, procédures et modes opératoires en vigueur dans l'établissement ;
* les documents de portée régionale et nationale mis à disposition par les instances régionales d’identitovigilance.

### Gestion des habilitations

Objet du chapitre : préciser les principes retenus par l'établissement 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 l’établissement…).

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.

### 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 nécessaires 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. 4.1.1).

### 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 l’établissement possèdent un dispositif d’enregistrement horodaté des accès précisant le nom (*login*), le type d’accès (lecture ou écriture) et les pages visitées. En application de l’article R6113-9-2 du code de la santé publique, la traçabilité des actions (création, modification et consultation) sont conservées pendant au moins 6 mois.

L’accès à ces informations n’est autorisé qu’à un nombre réduit de professionnels (directeur, DSI, responsable de l’instance opérationnelle). 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. 4.1.1).

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).

### 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 intègre les informations relatives à la gestion de l’identité de l’usager et rappelle ses droits vis-à-vis de ses données personnelles. Il précise l’importance d’une identification fiable, de sa participation à une bonne identification primaire et secondaire, et de la nécessité de disposer de documents à haut niveau de confiance permettant de confirmer son identité. Des informations sont également diffusées sur les écrans mis en place au niveau des admissions.

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

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

### 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.

## Gestion des risques *a posteriori*

### 4.2.1 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. 4.1.1) 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, plaintes et réclamations…

### 4.2.2 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 :

L’établissement met en place un système de signalement des événements indésirables piloté par la CQGR. Il promeut son emploi par l’ensemble des professionnels 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 (« MEDILAB », « RADIOSARL », médecins traitants, autres professionnels de santé) pour qu’ils lui signalent les anomalies constatées sur l’identification des usagers.

Les acteurs de santé impactés par la diffusion d’une erreur en lien avec l’identité INS sont alertés sans délais, selon une procédure spécifique formalisée par l'établissement.

L'instance opérationnelle, 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 en lien avec l’identitovigilance est renseignée, celle-ci est transmise à la CQGR qui émet un accusé de réception et signale sa transmission à l’instance opérationnelle pour traitement.

L’instance opérationnelle est chargée, en relation avec les professionnels concernés, de prendre part au retour d’expérience (REX) et à la mise en œuvre des actions correctrices (cf. 4.2.3 et 4.2.4).

Le signalement des événements indésirables liés à des erreurs d’identification est réalisé conformément aux règles définies dans l’établissement.

Il est important que tout difficulté rencontrée pour la récupération de l’identité INS ou la qualification de l’identité numérique, du fait d’une incohérence non mineure, soient signalée comme événement indésirable et rapportée au niveau régional et national. Ces modalités de signalement aux niveaux régional et national seront précisées ultérieurement.

### 4.2.3 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. 4.2.2), l’instance opérationnelle 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, l’instance opérationnelle met à disposition dans la GED (cf. 4.1.1) 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 l’instance opérationnelle lorsqu’un événement indésirable est associé à une mauvaise gestion de l’identité.

Ces informations enrichissent une base de données tenue par l’instance opérationnelle. Elle sert à la formation et à la sensibilisation des professionnels ainsi qu’à la mise à jour régulière des indicateurs de suivi (cf. 4.2.5).

### 4.2.4 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 :

L’instance opérationnelle est chargée de s’assurer régulièrement de la qualité de la base de données des identités de chaque domaine d’identification présents au sein de l’établissement.

Des procédures et modes opératoires, consultables dans la GED (cf.  4.1.1) 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.

### 4.2.5 Indicateurs de suivi

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

Exemple de rédaction :

L’instance opérationnelle 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 usagers. 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 l’instance opérationnelle (à titre indicatif) :

* nombre de signalements reçus en lien avec l’identitovigilance ;
* taux de doublons et collisions 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…

# Références réglementaires et techniques

Objet du chapitre : l’établissement renseigne ici les références réglementaires et techniques du présent document (exemple : RNIV ; instructions ; modèle régional de charte d’identitovigilance des établissements de santé…).

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). [↑](#footnote-ref-1)
2. *Object identifier* : identifiant numérique spécifique associé au matricule INS qui permet de distinguer sa nature : NIR ou NIA [↑](#footnote-ref-2)