FIP 07	Fiche pratique	Version 1 Janvier 2021

Conduite à tenir lors de la mise en évidence d'une discordance entre l'identité numérique et l'identité physique d'un usager

RÉSEAU DES
RÉFÉRENTS RÉGIONAUX
D'IDENTITOVIGILANCE

CONTRIBUTEURS

Structures de santé

Mme Marie CASTAGNE, Mutualité Française Limousine (SSR et EHPAD)

Mme Stéphanie COUDERT, HAD Santé Service Limousin

Mme Claire WEISS, Polyclinique privée Limoges

Dr Laïla BENMOUSSA, CHU Limoges

GT cas particuliers 3RIV

Mme Céline DESCAMPS, CRIV NA

Dr Christine LECLERCQ, GRADeS Occitanie (e-santé Occitanie)

Dr Isabelle MARECHAL, CHU Rouen

Mme Corinne MIGOT, EFS

Mme Christelle NOZIERE, CRIV NA

Dr Manuela OLIVER, GRADeS PACA (ieSS)

M. Loïc PANISSE, GRADeS Occitanie (e-santé Occitanie)

M. Bertrand PINEAU, GRADeS IDF (SESAN)

Dr Bernard TABUTEAU, CRIV NA

TABLE DES MATIÈRES

1 Introduction

Comme le rappelle le *Référentiel national d'identitovigilance* (RNIV 1 dit socle), la qualité de l'identification des usagers est une donnée fondamentale pour la qualité et la sécurité des parcours de santé. Elle constitue l'un des éléments de la confiance nécessaire au développement et à l'utilisation des services numériques dans les champs de la santé et du médico-social.

Le risque qu'un professionnel soit un jour confronté à une discordance avérée entre l'identité numérique utilisée et l'identité réelle de l'usager n'est pas nul. Ce professionnel doit avoir été sensibilisé à la détection de ce type d'anomalie, savoir en apprécier les dangers – notamment en termes de collision de données et d'erreur de décision, fondée sur des bases erronées – et connaître, s'il y est confronté, les modalités de correction voire de signalement si l'erreur est associée à un événement indésirable associé aux soins…

L'objet de cette fiche pratique est de définir une liste non exhaustive de situations où l'identité numérique utilisée se révèle différente de l'identité de la personne physique prise en charge et de proposer une conduite à tenir selon les conséquences identifiées.

Comme dans le RNIV socle, le terme « acteurs de santé » fait référence, dans ce document, aux établissements et professionnels de santé et du secteur médico-social, quel que soit leur mode d'exercice : hospitalier, ville, coordination des parcours, salarié ou libéral…

2 Les situations à risque

Les acteurs de santé utilisent de multiples outils numériques pour tracer, échanger et partager des données de santé : dossier de soins, applications métier, plateformes et outils numériques, dossier pharmaceutique, dossier médical partagé, etc. Ces usages augmentent le nombre de situations à risque de discordances entre l'identité numérique affichée par l'application informatique utilisée – ou un document imprimé référencé avec ses traits d'indentification – et l'identité réelle de l'usager physique pris en charge.

L'erreur, ou sa mise en évidence, peut se produire à n'importe quel moment du processus d'identification de l'usager :

- dès son accueil ;
- lors de la vérification des données en « back-office ;
- au moment de la consultation du dossier de l'usager ;
- lors de la transmission de données par voie numérique, postale ou remises directement à l'usager ou à son accompagnant dans le cadre d'une consultation, d'une sortie ou d'un transfert (fiche de liaison).

Cette erreur peut impacter les différentes phases de la prise en charge sanitaire : demande d'examen, administration d'un soin, acte opératoire, classement de résultats…

Les principales sources d'erreurs sont détaillées dans les chapitres suivants.

2.1 Erreur d'identification primaire à l'accueil de l'usager

Lors de l'accueil administratif d'un usager, plusieurs situations peuvent entraîner l'attribution incorrecte d'une identité numérique :

- par absence d'application des bonnes pratiques ;
- par sélection erronée d'une identité approchante ;

- à l'occasion de l'utilisation frauduleuse de l'identité d'un autre usager déjà enregistré dans la base de la structure, qui n'est pas détectée ;
- par erreur d'attribution d'une identité INS à un usager (acceptation des traits renvoyés par le téléservice, sans contrôle de cohérence avec celles de la personne prise en charge).

2.2 Modification de l'identité numérique après l'accueil initial

Il peut arriver qu'une modification des traits de l'identité numérique soit réalisée dans un deuxième temps alors que la prise en charge de l'usager a commencé. Elle est en général justifiée par la correction d'une erreur de saisie sur les traits d'identité initialement recueillis ou par la mise à jour de l'identité numérique après prise en compte d'une pièce d'identité officielle de haut niveau de confiance, non présentée au début de la prise en charge de l'usager ou récupération secondaire de l'identité INS. La réalisation de ces opérations *a posteriori* (en « back-office ») par un professionnel habilité ne constitue pas, en elle-même, une anomalie et peut, au contraire, refléter une maturité particulière de la structure en termes d'identitovigilance.

La mise à jour des traits d'identité se propage dans l'ensemble des logiciels rattachés au domaine d'identification (le référentiel d'identité de la structure), par le bais des messages d'interopérabilité mais également à d'autres acteurs non rattachés au domaine d'identification (demande d'examen pour les acteurs de santé sous-traitants, par exemple). Elle est toutefois susceptible, selon le moment où elle est réalisée, d'entraîner une discordance entre les traits d'identité initialement utilisés pour la prise en charge (étiquettes, demandes et résultats d'examens…) et ceux qui apparaissent ou sont imprimés après que la modification a été effectuée.

2.3 Erreur d'identification secondaire

Les erreurs les plus fréquentes sont liées à des défauts de pratique en termes d'identification secondaire, conduisant à réaliser le soin au mauvais patient ou à attribuer les données dans le mauvais dossier. Par exemple :

- réalisation d'un soin au mauvais patient par absence de contrôle de l'identité (administration médicamenteuse, prélèvement sanguin, examen radiologique…)
- prise en charge sans contrôle de l'usager qui arrive mais qui n'est pas celui attendu (mauvais choix du brancardier, changement de programme, usager non communiquant…) ;
- erreur de choix de dossier au cours de la prise en charge (identité approchante, erreur de recherche et de sélection, inattention…), que ce soit pour les soins, l'étiquetage, l'enregistrement de données informatiques ou le rangement de documents dans le dossier papier (résultats d'examens, comptes rendus, prescriptions médicales…) ;
- transmission de données inappropriées à un professionnel de santé (avec les mêmes sources que les dysfonctionnements précédents).

3 Les conséquences potentielles

Ce chapitre dresse une liste non exhaustive des conséquences potentielles des situations évoquées dans le chapitre précédent. Elles sont susceptibles d'affecter la qualité des parcours et la sécurité de l'usager de façon différente selon le moment où le dysfonctionnement se produit.

3.1 Identifications différentes pour un même usager en cours de séjour

Lorsque l'identité numérique est modifiée après le début de la prise en charge effective de l'usager par un professionnel de santé cela crée une discordance entre les nouveaux traits d'identité et ceux utilisés antérieurement lors d'acte de soins ou d'une demande d'examen à un prestataire externe (radiologie, analyse biologique…).

La discordance entre les traits d'identité initialement utilisés (bracelet d'identification, étiquettes, documents imprimés…) et la nouvelle identité numérique affichée sur les applications informatiques en temps réel amène à gérer des identités numériques différentes pour un même usager avec :

- la difficulté de prendre en compte les modifications après que les soins ont débuté, notamment en cas d'intervention chirurgicale, transfusion, chimiothérapie ou radiothérapie ;
- le risque d'entraîner la création de dossiers en doublons – notamment par le sous-traitant à qui sont transmises des demandes d'examen avec des identités modifiées – et d'avoir alors une vision incomplète de l'historique de la prise en charge.

Ces anomalies peuvent être à l'origine d'une perte de chance pour le patient du fait d'un retard de soin, d'une mauvaise décision thérapeutique, d'un défaut de rattachement automatique des résultats d'actes dans le dossier de l'usager…

3.2 Identifications différentes pour un même usager après son départ

La situation est un peu différente de la précédente dans le sens où tous les soins réalisés au cours du séjour ont théoriquement été bien rattachés au dossier de l'usager avec l'identité initialement recueillie. Les données informatiques du domaine d'identification sont donc mises à jour avec la nouvelle identité.

La correction de l'identité après le départ de l'usager impacte, comme dans le cas précédent, les systèmes d'information et les professionnels de santé qui ne sont pas informés des changements. Elle entraîne une discordance *a posteriori* sur tout ce qui n'a pu être mis à jour : courrier imprimé, données de santé transmises informatiquement à un acteur de santé qui ne fait pas partie de la boucle d'information, réception de résultats d'examens ou d'expertise demandés avec l'identité connue en cours de séjour.

Comme dans la situation précédente, elle est susceptible d'impacter le bon rattachement de résultats à l'usager et la qualité de la poursuite de la prise en charge.

3.3 Défaut de rapprochement des identités numériques

Toute discordance dans les traits d'identification peut avoir des impacts sur les échanges d'information entre applications qui ne partagent pas le même référentiel d'identités, lors de l'utilisation d'applications d'échange et de partage de données entre structures de santé et des rapprochements d'identités via des serveurs de rapprochements locaux, territoriaux ou régionaux.

Elle est à l'origine de la création de doublons de dossiers et représente un frein à la coordination des soins, notamment par la difficulté de retrouver l'historique exhaustif des prises en charge réalisées dans le parcours de soin de l'usager.

3.4 Collision entre les données d'usagers différents

La collision consiste à inscrire ou utiliser des données d'un usager différent de celui qui est pris en charge. La plupart des défaillances en termes d'identification primaire ou secondaire décrites au chapitre 2 peuvent être à l'origine de collisions.

Cette situation aboutit à la prise en compte de données diagnostiques et/ou thérapeutiques qui appartiennent à un autre usager, ce qui peut que nuire à la qualité de la prise en charge de chacun des usagers concernés.

3.5 Propagation d'une identité erronée

Les erreurs d'identification réalisées dans une structure peuvent être propagées à d'autres professionnels, notamment par voie informatique. Elles sont susceptibles d'avoir les mêmes conséquences, à distance, sur la qualité et la sécurité des prises en charge réalisées par les acteurs de santé destinataires des informations.

4 La conduite à tenir

4.1 Actions préventives

Elles sont destinées à limiter les risques de survenue des anomalies citées et la gravité de leurs conséquences.

4.1.1 Procédures de recherche d'antériorité d'enregistrement de l'usager

Il est nécessaire de formaliser une procédure qui décrit les modalités de recherche d'antériorité d'enregistrement d'une identité numérique d'un usager avant toute création ou modification d'identité (par les professionnels habilités). Cette procédure a pour objet de limiter les risques liés à la création d'une identité numérique erronée ou à la création d'un doublon. Elle doit s'appuyer sur les bonnes pratiques du RNIV qui précise que la recherche peut être réalisée à partir :

- soit de la date de naissance, avec la possibilité d'affiner la recherche par la saisie, en sus, des tout premiers caractères du nom (de naissance ou utilisé) ou du prénom (de naissance ou utilisé) ;
- soit de tout ou partie de l'identité INS, après l'interrogation du téléservice INSi avec la carte Vitale, ce qui limite les erreurs de saisie manuelle.

4.1.2 Procédure de modification d'identité

La modification des traits d'identité dans le système d'information de la structure doit faire l'objet d'une procédure écrite qui, *a minima* :

- définit quels sont les professionnels habilités à effectuer cette modification ;
- décrit les mesures spécifiques à prendre lorsque cette modification est réalisée en dehors de l'accueil administratif initial, alors que l'usager est toujours présent dans l'établissement (par exemple : évaluer le moment opportun pour réaliser la modification en fonction des actes programmés, en cours, ou déjà réalisés…) ;
- prévoit les modalités pour diffuser une information rapide à toutes les parties prenantes potentielles afin d'éviter les conséquences décrites au § 3.1.

4.1.3 Procédure d'identification secondaire

Il est également nécessaire de formaliser, dans une procédure relative aux bonnes pratiques d'identification secondaire, les modalités relatives à la recherche et la sélection d'une identité numérique pour s'assurer de toujours disposer du bon dossier au bon moment.

La mise en application des recommandations de bonne pratique pour la vérification de la concordance entre les éléments du dossier et la personne physique concernée est une obligation professionnelle qui s'applique à toutes les étapes de la prise en charge sanitaire de l'usager. Les modalités de réalisation de ce contrôle doivent être formalisées en fonction des activités réalisées et régulièrement rappelées dans la structure.

Par exemple :

- demander par questions ouvertes à l'usager de décliner son identité avant tout acte de soin ou de transport (si l'usager est en capacité de le faire) ;
- vérifier la concordance entre le dossier, l'usager et les données inscrites sur les étiquettes, le bracelet d'identification, la demande d'examen, les résultats reçus…

4.1.4 Cas particulier des documents transmis par un tiers

Pour utiliser une identité de confiance, tous les acteurs de santé doivent respecter les règles d'identification établies par le RNIV, qu'il s'agisse d'une identité INS ou pas. Dans le cadre des acteurs de santé sous-traitants, il est conseillé de formaliser un contrat de confiance avec une clause prévoyant le respect du RNIV par chaque partie.

Dans le cas où le destinataire a des doutes sur la qualité de l'identité transmise, l'intégration des documents dans le dossier de l'usager doit être étudiée au cas par cas. Un appel téléphonique à la structure à l'origine de la demande est à privilégier chaque fois que possible.

Sauf cas dérogatoire, l'appel au téléservice de vérification est nécessaire lorsque l'identité INS adressée ne fait pas encore l'objet d'un statut *Identité récupérée* ou *Identité qualifiée* chez le récepteur.

4.1.5 Sensibilisation et formation des acteurs

Les professionnels doivent régulièrement être sensibilisés à l'importance des bonnes pratiques d'identitovigilance et à leur impact sur la qualité et la sécurité des soins.

De la même façon, il est nécessaire d'informer les usagers (verbalement, par affichage…) sur l'intérêt de ces pratiques et de les inciter à participer de façon active à la sécurité de leurs propres soins. Les conséquences de l'utilisation frauduleuse d'une identité – pour celui qui fraude et pour l'usager auquel on a emprunté les documents d'identité et/ou de couverture maladie – doivent également être affichées dans les structures potentiellement concernées par ce type de fraude.

4.2 Actions correctives

Elles sont destinées à corriger les anomalies constatées et à limiter les conséquences sur la qualité et la sécurité des soins.

4.2.1 Signalement d'une discordance

Quelle que soit la cause de la discordance constatée ou des mises à jour réalisées qui n'ont pas pu être propagées, il est important d'en réaliser un signalement rapide (téléphonie, mail, fax…) pour alerter l'ensemble des parties prenantes afin qu'ils puissent prendre des mesures appropriées.

Parmi ces mesures, on peut citer, en particulier, l'évaluation de la balance bénéfices-risques par les soignants selon le moment où cette information leur parvient, pour décider :

- soit de suspendre la réalisation de l'acte le temps de faire les corrections appropriées ;
- soit de poursuivre les soins commencés et de ne prendre en compte les modifications qu'*a posteriori*.

Cette alerte est à doubler si nécessaire d'une déclaration d'événement indésirable, en application de la procédure de signalement de l'établissement (cf. 4.3).

Il sera nécessaire de prévoir une formation complémentaire des personnels, **des personnels habilités à créer et modifier des identités,** si l'erreur est liée à une modification secondaire qui n'a pas été signalée en temps opportun.

4.2.2 Gestion de l'anomalie avant conséquence

Il est nécessaire de comprendre rapidement l'origine de l'anomalie afin de déterminer les actions correctives à conduire. En voici quelques exemples.

- Lorsqu'il s'agit d'une modification d'identité *a posteriori*, il faut répercuter le plus rapidement possible toutes les modifications sur les documents et dispositifs qui n'ont pas été automatiquement modifiés par la mise à jour : réédition des étiquettes, modification de l'identité du bracelet, réédition des documents imprimés ou identification à l'aide du nouveau jeu d'étiquettes, etc... Il appartient à la structure de santé de définir une procédure sur les modalités à suivre dans ce cas-là.
- Lorsque c'est une erreur liée à la sélection du dossier ou à l'arrivée d'un patient qui n'est pas celui attendu, il faut bien entendu prendre les mesures permettant de revenir à une situation normale.
- Lorsque le doute lié à la discordance constatée ne peut être rapidement levé – cela concerne tout particulièrement les prestataires externes chargés de réaliser un examen demandé par la structure de santé – il est conseillé de créer un nouveau dossier pour éviter la collision de données non compatibles en attendant que le type d'anomalie soit identifié. La fusion des 2 dossiers pourra être réalisée dans un second temps avec les bons traits d'identification s'il s'avère que l'usager était bien le même.

Si c'est l'identité réelle de la personne qui est mise en doute, il faut appliquer la procédure sur la conduite à tenir lorsqu'on suspecte l'utilisation d'une identité frauduleuse (cf. Fiche pratique FIP 05 « conduite à tenir lorsqu'on suspecte l'utilisation d'une identité frauduleuse » publiée par le 3RIV).

La découverte d'une anomalie fait l'objet d'une déclaration d'événement indésirable dans les cas prévus par la procédure locale (cf. 4.3).

4.2.3 Gestion des conséquences de l'anomalie

La découverte de l'anomalie peut être postérieure à l'acte de soins ou la mise à jour du dossier. Dans tous les cas l'anomalie doit être corrigée dans le dossier selon une procédure qui doit être formalisée par l'établissement. Elle précise qui a le droit de réaliser ce type d'opération et comment.

4.2.3.1 Démarche générale

Il faut dans tous les cas :

- communiquer l'information à tous les professionnels concernés par la diffusion de l'anomalie (internes et externes à la structure, y compris les responsables de traitement des applications territoriales ou régionales) de façon qu'ils évaluent à leur niveau les conséquences éventuelles de cette transmission ;
- rééditer et transmettre les documents corrigés, si applicable, à ces mêmes destinataires ;
- alerter les opérateurs sur le risque d'erreur du fait de l'emploi d'une identité numérique ayant des identités approchantes dans la base de données (intérêt de l'attribut *Identité homonyme* prévu par le RNIV) ;
- attribuer le statut *Identité provisoire* et l'attribut *Identité douteuse*, à l'identité numérique d'une personne suspecte d'utilisation frauduleuse de l'identité.

Les conséquences d'une erreur d'identitovigilance doivent faire l'objet d'une déclaration d'événement indésirable dans les conditions prévues par la politique de gestion des risques de l'établissement (cf. 4.3).

4.2.3.2 Cas où l'identité de l'usager auquel appartient la donnée est connue

Il convient de rattacher au(x) bon(s) usagers les données implémentées dans un mauvais dossier et celles qui n'ont pu être automatiquement attribuées au bon dossier du fait des modifications apportées secondairement.

4.2.3.3 Cas où l'identité de l'usager auquel appartient la donnée est inconnue

Il faut impérativement prévenir l'émetteur de la donnée (téléphonie, mail, fax…) afin que celui-ci puisse transmettre un rectificatif de l'identité dans les plus brefs délais. Cette alerte doit faire l'objet d'une trace écrite.

S'il n'est pas possible de la supprimer du dossier dans lequel elle a été intégrée par erreur (en fonction des possibilités des logiciels métiers), elle devra être précisée comme « Invalide » dans le dossier de l'usager, avec un commentaire qui en précise le motif.

Dans tous les cas, il est nécessaire d'alerter le référent en identitovigilance local.

4.3 Déclaration d'événement indésirable

Toutes les situations de discordance avérées peuvent être à l'origine d'une erreur de soins avec des conséquences plus ou moins graves (cf. *Fiche mémento sur la gestion des événements indésirables en identitovigilance* publiée par le 3RIV).

Que l'anomalie constatée ait eu ou non des conséquences, il est important que ce type d'erreur soit comptabilisé par la structure afin de mettre en œuvre, si besoin, des actions correctives : évolution des procédures, sensibilisation des professionnels, formations complémentaires… Cela passe donc par la déclaration d'un événement indésirable sur le système d'information déployé par la structure pour ce type de signalement. Il est également important que la structure identifie bien l'événement comme faisant partie des anomalies en rapport avec l'identitovigilance, même lorsque les conséquences concernent une autre vigilance indue.

La structure doit se conformer aux obligations réglementaires de déclaration externe de l'événement indésirable (EI), via :

- le portail national de signalement (EI en lien avec une vigilance réglementée, événement indésirable associé aux soins) ;
- le point focal de l'Agence régionale de santé (EI grave) ;
- le portail de télédéclaration de l'Agence de sécurité nucléaire (événement significatif de radioprotection).

Il peut être aussi important de signaler au référent régional en identitovigilance, en fonction des organisations régionales mises en place, tout événement utile à partager collectivement.