FIP 05	Fiche pratique	Version 1 Novembre 2020

Conduite à tenir lorsqu'on suspecte l'utilisation d'une identité frauduleuse

RÉSEAU DES
RÉFÉRENTS RÉGIONAUX
D'IDENTITOVIGILANCE

CONTRIBUTEURS

Dr Laila BENMOUSSA (CHU Limoges)

Mme Céline DESCAMPS (CRIV NA)

Mme Christelle NOZIERE (CRIV NA)

Dr Manuela OLIVER, GRADeS PACA (ieSS)

Dr Philippe SEJOURNE (CH Agen Nérac)

Dr Bernard TABUTEAU (CRIV NA)

TABLE DES MATIÈRES

1 Introduction

Comme le rappelle le *Référentiel national d'identitovigilance*, 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 des services numériques dans les champs de la santé et du médico-social.

L'objet de cette fiche est de définir la conduite à tenir lorsqu'une structure de santé suspecte que l'usager pris en charge se sert de l'identité d'une autre personne, notamment pour bénéficier de sa couverture sociale. L'utilisation frauduleuse d'une identité, consentie ou pas par un autre usager, met doublement en danger les personnes impliquées : les données de santé de chaque usager se mélangent (collision) dans le dossier patient utilisé et risquent de venir fausser la pertinence d'un diagnostic ou d'un traitement qui le concerne, soit dans l'immédiat, soit à l'occasion d'une prise en charge ultérieure.

Remarque : comme dans le RNIV, les termes « structure de santé » et "acteur de santé" font référence, dans ce document, aux établissements et professionnels de santé, quel que soit leur mode d'exercice : hospitalier, médico-social, ville, coordination des parcours, salarié ou libéral…

2 Définitions

Légalement, une *usurpation d'identité* correspond à l'utilisation délibérée de l'identité d'une autre personne à son insu, donc sans son consentement. Cette infraction est un délit réprimé par le code pénal (art. 226-4-1 et 434-23 du code pénal, cf. § 3).

Dans le monde sanitaire, il n'est pas rare de rencontrer des cas d'emprunt d'identité d'une autre personne afin de bénéficier de sa couverture sociale ou de droits particuliers[1] :

- soit avec la complicité de celui-ci ;
- soit par l'obtention frauduleuse d'une carte vitale.

Cette utilisation frauduleuse relève de la qualification pénale d'escroquerie (art. 313-1 *& suiv.* du code pénal, cf. 3).

Dans ce document, ces situations sont réunies sous une même appellation : utilisation d'une identité frauduleuse.

3 Références réglementaires

- **Article 226-4-1 du code pénal :** « Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. »
- **Article 313-1 du code pénal** : « L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au

[1] Pour exemple : utilisation par une mineure désirant avorter de la carte vitale d'une amie majeure pour être sûre que des parents ne l'apprendront pas

préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende. »

- **Article 313-2 du code pénal : «** Les peines sont portées à sept ans d'emprisonnement et à 750 000 euros d'amende lorsque l'escroquerie est réalisée :
  1° Par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission ;
  2° Par une personne qui prend indûment la qualité d'une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ;
  3° Par une personne qui fait appel au public en vue de l'émission de titres ou en vue de la collecte de fonds à des fins d'entraide humanitaire ou sociale ;
  4° Au préjudice d'une personne dont la particulière vulnérabilité, due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, est apparente ou connue de son auteur ;
  5° Au préjudice d'une personne publique, d'un organisme de protection sociale ou d'un organisme chargé d'une mission de service public, pour l'obtention d'une allocation, d'une prestation, d'un paiement ou d'un avantage indu.
  Les peines sont portées à dix ans d'emprisonnement et à 1 000 000 euros d'amende lorsque l'escroquerie est commise en bande organisée. »
- **Article 434-23 du code pénal :** « Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. »

4 Sur quels éléments soupçonner une usurpation d'identité ?

4.1 Lors de l'enregistrement de l'usager

Les bonnes pratiques d'identitovigilance prévoient que le professionnel qui reçoit un usager doit s'efforcer d'appliquer les exigences de l'identification primaire définies dans le RNIV 1.

Il peut être alerté sur la possibilité d'utilisation d'une identité frauduleuse par des anomalies telles que :

- certains traits de l'identité présentée ne correspondent pas à l'usager qui est face au professionnel (photographie, âge, taille…) ;
- l'usager est hésitant et ne répond pas de façon claire aux questions qui lui sont posées sur certains de ses traits (date et lieu de naissance, n° de téléphone, venues antérieures…) ;
- les documents utilisés ont un format inhabituel (carte d'identité ou passeport sans tampon officiel, format suspect des documents ou de la photographie, etc.).

4.2 Au cours de sa prise en charge

Des anomalies peuvent aussi apparaître secondairement, lorsqu'il est mis en évidence des incohérences dans les antécédents ou les résultats d'examens. Par exemples :

- femme enceinte qui a déjà accouchée 3 fois en 2 ans ;
- résultat de groupe sanguin incompatible avec le dossier transfusionnel préexistant ;
- cicatrice d'intervention non retrouvée ou inexpliquée…

Après avoir éliminé formellement une erreur de dossier, il faut alors envisager la possibilité d'utilisation d'une identité frauduleuse.

4.3 Après sa prise en charge

Dans d'autres situations, ce sont les informations reçues *a posteriori* qui peuvent amener à suspecter l'usage d'une identité frauduleuse. Pour exemples :

- réception de résultats non cohérents avec la prise en charge effectuée ;
- doutes émis par un autre professionnel ;
- aveu de l'usager lui-même ou de la personne qui lui avait « prêté » sa carte Vitale...

4.4 Remarque

Il existe des situations où les anomalies constatées ne sont pas révélatrices d'une volonté de fraude. Cela peut être le cas, pour exemple, lors de la prise en charge d'un usager confus ou incapable de décliner son identité alors qu'il est détenteur de documents d'identité non cohérents.

5 Quelle est la conduite à tenir immédiate ?

Les structures de santé susceptibles d'accueillir des usagers utilisant une identité frauduleuse – de façon volontaire ou non – doivent disposer de procédures opérationnelles adaptées. Pour exemples :

- accueil d'un usager incapable de décliner son identité ;
- accueil d'un usager avec suspicion d'utilisation frauduleuse de l'identité d'un autre.

Dans tous les cas, au moindre doute sur l'identité réelle d'un usager accueilli ou pris en charge, la règle est de tout faire pour ne pas risquer de mélanger les données qui lui sont propres et celles qui seraient présentes dans un dossier préexistant partageant les mêmes identifiants (risque de collision).

Ces précautions sont prises en fonction des possibilités du système d'information utilisé et des consignes en vigueur existant dans l'établissement. Une alerte immédiate des référents en identitovigilance de la structure, lorsqu'ils existent, est fortement recommandée.

5.1 Lors de l'enregistrement de l'usager « suspect »

Si aucun dossier n'existe pour l'identité alléguée, elle est créée de façon habituelle mais doit rester strictement en statut « Identité provisoire » tant que le doute persiste[2]. L'ajout d'un attribut supplémentaire « Identité douteuse » est souhaitable, si le système d'information le permet, de façon à pouvoir l'identifier comme à risque particulier.

Dans le cas où un dossier est retrouvé avec les mêmes identifiants, il est nécessaire de créer un nouveau dossier, selon la procédure en vigueur dans la structure, en refusant toute proposition de rapprochement entre les 2 identités tant que le doute n'a pas été levé. En fonction des possibilités locales du système d'information, il pourrait être décidé, par exemple, d'ajouter un caractère spécifique en suffixe au champ nom ou nom d'usage (comme un « ? » ou un « D »…) pour le différencier d'un homonyme et/ou de faire la mention explicite du doute dans un champ commentaire.

Cette disposition permet de réaliser les identifications secondaires en utilisant l'identité alléguée du patient, ce que ne permet pas les identités fictives commençant par « X SE DISANT… », par exemple.

[2] L'usage de certains établissements de valider « automatiquement » des identités provisoires au bout d'un certain délai, sans preuve documentaire, est une pratique à proscrire absolument (Exi PP 09, RNIV 1)

5.2 Au cours de sa prise en charge

Le risque, dans cette situation, c'est d'avoir commencé à saisir des données de santé dans le dossier du véritable usager dont l'identité est utilisée. Là encore, la mesure urgente à prendre est de demander la création d'un nouveau dossier, de façon à pouvoir le renseigner avec les données à venir. Ce nouveau dossier est à traiter comme au chapitre précédent, en le classant comme *Provisoire* et, si possible, comme *Douteux*.

Il est impératif de s'assurer que tous les acteurs concernés par la prise en charge (pharmacie, laboratoire, radiologie, EFS, médecin traitant…) sont bien informés du doute concernant l'identité et que les dispositions nécessaires seront prises à leur niveau pour limiter le risque de collision, selon des procédures qui leur sont propres.

Il est également impératif de vérifier que les modifications apportées ont bien été répercutées dans les différentes solutions informatiques concernées par la prise en charge de l'usager au sein de la structure.

5.3 Après sa prise en charge

Dans tous les cas, les dossiers classés avec des attributs *Provisoire* et *Douteux* doivent faire l'objet d'une enquête particulière (cf. 5.4).

S'il existe une collision avérée, il appartiendra aux référents en identitovigilance de la structure – ou au professionnel qui en tient lieu – de créer une nouvelle identité numérique (cf. 5.1) avec le statut *Identité provisoire* et l'attribut *Identité douteuse*. La procédure doit prévoir les modalités pratiques pour redistribuer les informations entre le dossier antérieur et le nouveau. Notamment :

- le motif des modifications doit être tracé dans les 2 dossiers ;
- les modifications concernant l'identification doivent être reportées sur l'ensemble des pièces du nouveau dossier (compte rendu opératoire, bilan sanguins, imagerie…) ;
- les éléments à risque particulier, comme la carte de groupe sanguin, doivent faire l'objet d'une attention particulière.

5.4 Compléments d'informations

La suspicion d'utilisation frauduleuse d'une identité doit, si possible, être étayée par un complément d'enquête. On peut imaginer, avec toutes les précautions oratoires que cela suppose, de :

- demander un complément de justificatifs à l'usager actuel : autres documents d'identité voire justificatif de domicile de type de facture de gaz ou d'électricité ;
- vérifier que le numéro de téléphone portable de l'usager correspond bien à celui qui était enregistré dans le dossier précédent, s'il existe ;
- rencontrer des proches pour venir confirmer les informations enregistrées (en leur demandant de répondre à des questions à voix haute, pas en demandant de certifier des écrits) ;
- etc.

Les professionnels n'ont toutefois pas à prendre la place des autorités de police qui seule a le droit de mener une enquête approfondie.

6 À qui signaler une suspicion de fraude ?

Le détail des mesures à prendre après que la suspicion de fraude est constatée doit être détaillé dans la procédure *ad hoc*.

6.1 En interne

Tout professionnel qui constate ou suspecte une fraude doit :
- informer les professionnels susceptibles de prendre en charge cet usager ;
- tracer cette information sur le dossier administratif et de soins ;
- alerter les professionnels et instances concernées (direction, cellule d'identitovigilance, département d'information médicale, service de facturation…)
- faire un signalement interne, via une fiche d'événement indésirable, afin de tracer le cas qui pourra faire l'objet d'un retour d'expérience *a posteriori*.

6.2 En externe

La direction de la structure ou ses représentants désignés sont invités à :
- déposer une plainte auprès du commissariat de police ou du procureur pour suspicion d'escroquerie (article 40 et suivants du code de procédure pénale) ;
- alerter les organismes de sécurité sociale de ce dépôt de plainte.

7 Quelles autres mesures préconiser ?

Il est important de prévoir de contacter les parties concernées par cet emprunt d'identité afin de les informer des conséquences et dangers liés à cette pratique. Cela concerne :
- celui ou celle qui a utilisé une identité qui n'était pas la sienne – pour l'informer notamment qu'il doit s'acquitter de tous les frais relatifs à son séjour et pour l'aider à régulariser sa situation au regard de ses droits sociaux, si applicable ;
- celui ou celle dont l'identité a été utilisée à tort – afin qu'il puisse faire valoir ses droits, s'il le souhaite ;
- celui ou celle qui a permis ou préconisé l'usurpation – pour l'informer des risques encourus personnellement sur le plan juridique.

Une information par voie d'affichage sur les dangers de l'utilisation frauduleuse d'une identité et sur les sanctions pénales doit être mise en œuvre par les structures concernées afin de diminuer les situations récurrentes de fraude.