

Foire aux questions sur l'identification en santé mentale

CONTRIBUTEURS

Membres du groupe de travail « identification en santé mentale »

- Mme Nathalie AGOGUE (Dir soins CH Dax)
- Mme Annabelle ANDANSON (Cadre adm CHPE)
- M. Jean-Luc ANGER (Resp bureau entrée CH Gérard Marchand)
- Dr Catherine BALLAY (DIM CHPE)
- Dr Fabien JOUBERT (DIM CH Le Vinatier)
- Dr Véronique LANGLOIS-GEY (DIM CH Esquirol)
- Dr Olessya LAURENT (DIM CH Georges Sand)
- Dr Florence LEYMARIE (DIM CH Gérard Marchand)
- Mme Christelle NOZIÈRE (CRIV NA)
- Dr Philippe PARADIS (DIM EPSM des Flandres)
- Mme Catherine PATEAUD (Cadre de santé CHPE)
- M. Laurent PLAS (DAG CH Camille Claudel)
- M. Lionel RIELLO (DSI CH Charles Perrens)
- Dr Bénédicte SOULA (DIM CH des Pyrénées)
- Dr Bernard TABUTEAU (CRIV NA)

TABLE DES MATIÈRES

1	Comment créer une identité numérique en situation dégradée ?	1
2	Quel niveau de confiance attribuer à l'identité numérique créée ?	2
3	Qui peut interroger le téléservice INSi ?	3
4	Doit-on enregistrer les nom et prénom utilisés ?	3
5	Comment accéder à un dossier informatique en urgence ?	3

1 Comment créer une identité numérique en situation dégradée ?

Il arrive souvent que les conditions d'identification ne soient pas idéales, soit parce que l'on reçoit des patients incapables de décliner correctement leur identité, soit parce qu'ils ne sont pas porteurs d'un document d'identité, soit parce qu'il semble légitime de douter de la réalité de l'identité annoncée ou présentée. En santé mentale, il est également fréquent que les professionnels qui accueillent les patients, notamment dans les sites de consultation déportée, ne soient pas en mesure de réaliser correctement cette identification pour des raisons techniques : manque de temps, absence de formation aux bonnes pratiques d'identification, absence d'accès direct au référentiel d'identités de la structure mère...

Le référentiel national d'identitovigilance (RNIV) stipule que la création d'une identité numérique requiert la saisie d'une information dans au moins 5 traits stricts (Exi PP 02) : nom de naissance, premier prénom de naissance, date de naissance, sexe et lieu de naissance. Cette identification doit être réalisée avant toute prise en charge de façon à pouvoir tracer la prise en charge effectuée.

Plusieurs situations peuvent être rencontrées.

➤ **Le patient est connu et possède déjà un dossier**

Sauf si la structure le rend obligatoire, il n'est pas obligatoire de contrôler systématiquement l'identité d'un patient connu. Il faut surtout s'assurer d'utiliser le bon dossier en le recherchant avec une méthode appropriée qui passe par l'utilisation systématique de la date de naissance comme filtre de recherche principal, associée si besoin aux premières lettres du nom ou du prénom. Dans le doute, il faut quelques fois créer un nouveau dossier pour éviter le risque de collision de données.

➤ **La création d'une identité par appel au téléservice INSi est possible**

La solution la plus simple, sous réserve d'avoir accès à la carte Vitale du patient de posséder une carte d'authentification de type CPx, est de faire appel au téléservice INSi pour récupérer directement l'identité INS. Les traits stricts sont alors automatiquement récupérés dès lors que l'opérateur valide le fait que les traits affichés par le téléservice correspondent bien au patient pris en charge. L'identité numérique ainsi recueillie est par défaut au statut *Identité récupérée*. Le titre d'identité doit si possible être scanné ou photographié et adressé aux professionnels habilités à gérer les identités : bureau des entrées, service des admissions... Ils se chargeront *a posteriori* des vérifications d'usage et de l'amélioration, si possible, du niveau de confiance de l'identité numérique (cf.2).

➤ **L'identification avec un document d'identité est possible mais réalisée *a minima*.**

Seuls les 5 traits stricts obligatoires sont recueillis à partir du document d'identité présenté. L'identité numérique est par défaut au statut *Identité provisoire*. Comme dans le cas précédent, les contrôles

nécessaires à l'attribution d'un statut de confiance de l'identité numérique peuvent être délégués aux professionnels habilités avec, si possible, la copie du titre d'identité (cf.2).

➤ **L'identification est réalisée à l'aide des informations transmises par un acteur de santé**

Lorsque le patient est adressé par un professionnel, il est possible de se servir des traits affichés sur le document de liaison ou transmis par voie électronique, en les complétant au besoin avec les éléments fournis par le patient ou relevés sur une pièce d'identité. L'identité numérique est par défaut au statut *Identité provisoire*. Comme dans le cas précédent, les contrôles nécessaires à l'attribution d'un statut de confiance de l'identité numérique peuvent être délégués aux professionnels habilités avec, si possible, la copie du titre d'identité (cf.2).

➤ **L'identification est possible mais sans document d'identité**

Le recueil des traits stricts est réalisé « aux dires du patient » en complétant si besoin les données manquantes (exemple : 99999 pour le champ lieu de naissance). L'identité numérique est par défaut au statut *Identité provisoire*. Comme dans le cas précédent, les contrôles nécessaires à l'attribution d'un statut de confiance de l'identité numérique peuvent être délégués aux professionnels habilités avec, si possible, la copie du titre d'identité (cf.2).

➤ **L'identification est impossible**

Il est alors nécessaire d'attribuer une identité fictive au patient, selon une procédure prévue par la structure, afin de renseigner les 5 champs obligatoires : nom et prénom fictifs, date de naissance au 31/12 d'une année compatible avec l'âge estimé du patient, sexe réel, lieu de naissance codé en 99999. L'identité numérique est par défaut au statut *Identité provisoire* et, si le système d'information le permet, il est utile de signaler son côté fictif à l'aide de l'attribut *Identité fictive*.

➤ **Dans tous les cas**

S'il existe le moindre doute sur une incohérence entre l'identité recueillie et celle du patient pris en charge, il est nécessaire de créer une identité numérique en lui attribuant, si le système d'information le permet, l'attribut *Identité douteuse*.

2 Quel niveau de confiance attribuer à l'identité numérique créée ?

L'attribution d'un niveau de confiance à toute identité numérique créée est obligatoire (Exi SI 07). Le statut se déduit de 2 facteurs :

- la possibilité de récupérer ou vérifier l'identité INS par le biais du téléservice INSi
- la possibilité de contrôler la cohérence entre les traits de l'identité numérique et ceux portés par un document d'identité de haut niveau de confiance : passeport ou carte nationale d'identité.



Dans les conditions normales d'identification, les personnels de l'accueil ont la possibilité de réaliser ces 2 opérations en une ou plusieurs fois et d'attribuer le statut de confiance *ad hoc*.

Dans les situations où l'identification est réalisée dans des conditions dégradées (cf. 1), le statut de l'identité numérique est le plus souvent, par défaut, *Identité provisoire*. Les modifications de l'identité numérique et du statut interviendront secondairement selon que les personnels habilités auront pu :

- accéder au téléservice INSi (cf. 3)
 - o soit pour recueillir l'identité INS du patient,
 - o soit pour vérifier une identité INS transmise par un acteur de santé externe ;
- effectué un contrôle de cohérence des traits à l'aide d'un document de haut niveau de confiance.

Lorsque le patient est déjà connu dans la structure, il est possible que les conditions dégradée d'identification conduise à la création d'un ou plusieurs dossiers en doublon le concernant. Le rapprochement avec une identité numérique préexistante pourra éventuellement se faire *a posteriori* par des professionnels spécialement habilités (cellule d'identitovigilance), en récupérant le statut de l'identité numérique ayant le plus haut niveau de confiance.

3 Qui peut interroger le téléservice INSi ?

Il appartient à chaque établissement de santé de définir quels sont les professionnels habilités à interroger le téléservice INSi. À ce jour, ceux-ci doivent détenir une carte CPx nominative pour s'authentifier auprès du téléservice INSi.

Le rapport bénéfice - risques doit être évalué pour chaque cas, en fonction des organisations et contraintes internes : établissement multisites, points de consultation déportés sans personnel administratif formé à l'accueil, absence de liaison informatique entre le site distant et l'établissement de référence...

Les solutions retenues doivent être décrites dans la charte d'identitovigilance (Exi PP 15) voire dans la cartographie applicative pour les systèmes d'information distants (Exi PP 12). Des procédures doivent être élaborées pour préciser les conditions de création ou modification d'identité dans les situations normales et dégradées.

4 Doit-on enregistrer les nom et prénom utilisés ?

L'enregistrement du nom et du prénom utilisé (s) est obligatoire lorsqu'ils sont différents, respectivement, du nom de naissance ou du premier prénom d'état civil (Exi PP 17 et 18).

Ces traits d'identités, non officiels, ont pour objet de faciliter la prise en charge des usagers qui n'utilisent pas dans la vie courante l'identité officielle (et notamment les traits INS). Leur utilisation en santé mentale peut être utile pour renseigner et respecter l'identité utilisée par les patients, même si elle fantaisiste.

Il appartient à chaque structure de définir sa politique d'enregistrement et de modification de ces champs en fonction des besoins. Comme cela est précisé dans le RNIV, elle peut rendre leur utilisation obligatoire dans tous les cas.

5 Comment accéder à un dossier informatique en urgence ?

Seuls les professionnels qui prennent en charge le patient ont réglementairement accès à son dossier. Mais il arrive régulièrement qu'un personnel soignant qui ne faisait pas partie de ce « cercle de confiance » ait besoin d'accéder à tout ou partie des données de santé du patient.

Il est tout à fait possible de modifier les droits informatiques d'un professionnel qui entre dans le cercle de confiance pour lui donner cet accès, notamment quand c'est une opération programmée (remplacement, nouvelle arrivée dans un service...). Dans le cadre de l'urgence, il est nécessaire de prévoir une procédure

dite « bris de glace » pour permettre un accès aux informations vitales pour la continuité de la prise en charge du patient (Reco ES 01).

La politique d'accessibilité aux applications gérant des données personnelles est à formaliser par chaque structure dans une charte informatique (Exi PP 13). Le système d'information doit garder la trace des accès aux informations protégées en précisant *a minima* qui et quand.

6 Peut-on utiliser 2 référentiels d'identités dans un même établissement ?

Il n'est pas rare, notamment dans les établissements de santé mentale, d'avoir des logiciels séparés assurant l'identification des usagers pris en charge : le référentiel d'identités officiel de la structure, rattaché au dossier patient utilisé lors des hospitalisations, et celui utilisé essentiellement dans le cadre des consultations, notamment lorsqu'elles sont déportées. Avec parfois 2 niveaux différents d'exigences en termes d'identitovigilance : des règles strictes pour l'hospitalisation et des pratiques variables pour les consultations.

Ces dispositions ne correspondent pas aux exigences actuelles en termes de qualité et de sécurité de l'identification primaire des usagers qui stipulent que dans un même établissement il ne doit y avoir :

- qu'une seule base maître d'identités, appelée référentiel d'identités (Exi SI 13 du RNIV) afin d'assurer la cohérence des identités numériques dans l'ensemble des logiciels utilisés par la structure ;
- qu'une même procédure d'identification primaire opposable à l'ensemble des professionnels de la structure.

Si rien n'empêche, théoriquement, l'établissement de gérer une base d'identités annexe (esclave) dédiée à l'activité ambulatoire, c'est uniquement sous réserve de l'absence de dégradation de la sécurité des échanges. La qualité de la liaison bidirectionnelle entre les 2 bases (ou le rapprochement des identités) est de la responsabilité du directeur d'établissement et du responsable du SI : ils doivent garantir l'absence de tout écart (Exi PP 12) et la bonne gestion de l'identification par tous les personnels qui y ont accès (Exi PP 13).

Dans la réalité, les interfaces ne sont jamais totalement maîtrisées (écarts entre les champs d'identités, leur longueur, qualité des flux d'interopérabilité...). Mieux vaut donc s'organiser pour que la saisie des identités se fasse sur une seule base partagée par tous, sous couvert de procédures appropriée (cf. 1).

Le référentiel d'identités doit être géré au niveau le plus élevé dans la hiérarchie des applications gérant des identités patient utilisées par la structure. Il est le seul à pouvoir attribuer les statuts des identités numériques avec des professionnels spécialement formés et habilités à accéder au téléservice INSi, dans les conditions fixées par le RNIV. Il en est de même pour la réalisation périodique des audits qualité du référentiel et la gestion des doublons et collisions. Il est également le seul à pouvoir gérer en toute sécurité les appels au téléservice INSi pour la vérification des identités INS enregistrées dans le référentiel, à programmer tous les 3 à 5 ans, en application du référentiel INS.