FICHE 7

Les modalités de gestion des identités patients

Cette fiche technique présente un exemple de mise en œuvre de gestion des identités patients dans le cadre d'un GHT. Cet exemple s'appuie sur la gestion des rendez-vous et présente le rôle central du serveur d'identité unique à mettre en place pour le rapprochement des identités.

Principes de gestion de l'identité patient

Dans tous les cas, comme l'exigent les prérequis du programme Hôpital numérique, le référentiel d'identité des patients doit être unique.

Procédures au sein de chaque établissement du GHT

Chaque structure de santé doit rédiger, tenir à jour et appliquer au minimum les procédures suivantes :

- organisation de l'identitovigilance au sein de l'établissement. Cette procédure, ou charte de fonctionnement, décrit les structures mises en place au niveau de l'établissement;
- procédure de gestion et de contrôle qualité des bases d'identités des professionnels de santé comprenant la procédure de déclaration d'un nouvel agent au sein du SIH et la définition des droits d'accès (cette procédure intégrera la gestion des clôtures de compte);
- procédure d'identification primaire à l'accueil du patient dans l'établissement;
- procédure d'identification du patient dans un contexte d'urgence et hors heures ouvrables;
- procédure de correction et de rapprochement d'identité (fusion) dans le SIH ;
- procédure de correction et de rapprochement d'identité (fusion) dans les logiciels périphériques si nécessaire;
- procédure de recherche de patient dans la base ;
- procédure d'admission pour les patients à l'identité non connue ;
- procédure d'admission pour les patients souhaitant garder l'anonymat;
- procédure d'identification secondaire du patient avant tout acte de soin ;
- procédure de gestion et de contrôle qualité des bases d'identités patients ;
- procédure dégradée de fonctionnement permettant l'identification primaire et secondaire lors de panne du système d'information hospitalier ;
- procédures liées à l'utilisation d'un bracelet d'identification (si pertinent selon le type d'établissement);
- procédure de gestion des identités dans les logiciels au cœur du processus de soin non ou incomplètement interfacés.

CARACTÉRISTIQUES DE L'IDENTIFIANT NATIONAL DE SANTÉ (INS)

L'identifiant national de santé (INS) sert d'identifiant fédérateur pour le rapprochement de domaines d'identification. Toutefois, les applications métiers actuellement utilisées ont leur propre identifiant du patient et continueront de l'utiliser ; l'INS est donc ajouté comme un nouveau trait « strict » du patient.

Un INS est attribué à chaque bénéficiaire de l'assurance maladie. En application de l'avis de la Cnil du 20 février 2007, l'INS doit être :

- unique : un seul INS pour chaque personne tout au long de sa vie ;
- non signifiant : la connaissance de l'INS ne doit pas permettre de déduire des informations sur la personne ;
- sans doublon ni collision.

L'INS n'est ni public ni secret : il est privé, c'est une information personnelle du patient, protégée par la loi Informatique et libertés, au même titre que le nom et le prénom.

L'INS n'est pas porteur en soi de sécurité, c'est la procédure d'authentification qui associe un individu à un identifiant qui concourt à la sécurité.

Afin de respecter pleinement les caractéristiques attendues, la cible est la mise à disposition d'un INS généré aléatoirement (INS-A) et automatiquement par un système centralisé, dès l'inscription du numéro de la personne dans le Répertoire national informatisé de l'assurance maladie (RNIAM). Cet INS-A sera inscrit, à terme, dans la puce électronique de la carte Vitale du patient.

Pour répondre aux besoins à court terme et ne pas pénaliser le déploiement des systèmes de santé partagés, un INS provisoire dit « calculé » (INS-C) est utilisé. Il peut être calculé localement dans tout système d'information de santé en appliquant un algorithme connu de tous les acteurs sur un nombre réduit de traits d'identité extraits de la carte Vitale du patient. Le choix des traits utilisés (numéro d'inscription au répertoire [NIR], prénom et date de naissance) vise à limiter le risque de doublon dans la mesure où ces traits sont parmi les plus invariables de la personne. Un risque minime, et assumé, de collision demeure, il est lié au processus mathématique et minimisé par le choix de l'algorithme étudié en coopération avec les experts de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Ce mode de calcul ne permet pas aujourd'hui d'obtenir un INS pour les mineurs de moins de 16 ans et les ayants droit majeurs dont le NIR n'est pas renseigné dans la carte Vitale de l'ouvrant droit. Aujourd'hui, l'INS ne peut être calculé pour tous les patients.

L'Asip Santé a publié le *Référentiel d'identification des patients – Volet INS-C*, télé- chargeable à partir du site :

http://esante.gouv.fr/services/referentiels/identification/referentiels-d-identification

Ce référentiel d'identification contient les spécifications de l'algorithme de calcul de l'INS-C ainsi que les aspects juridiques associés.

Programme Hôpital numérique : l'intégration de l'INS dans le référentiel unique d'identité du patient et la mise en œuvre d'une cellule d'identitovigilance sont des prérequis (http://www.sante.gouv.fr/programme-hopital-numerique.html).

Gestion des identités patients

Exemple de la gestion des rendez-vous

Une solution de gestion des rendez-vous et de planification des ressources (GDR) doit s'articuler avec la gestion des identités des patients, voire de leurs venues quand elle intègre la planification des hospitalisations. Cela se traduit par une interface avec le système de gestion administrative des malades (GAM) ou des patients (GAP), classiquement référent du SIH pour la gestion des identités et des mouvements (donc des hospitalisations) ou, pour les établissements qui se sont dotés d'un serveur d'identités patients, par une interface avec ce serveur.

Note

Le terme anglo-saxon consacré pour «serveur d'identités patients» est *master patient index*, dont l'acronyme, tout aussi consacré, est MPI. Il n'y a pas encore d'acronyme consacré pour la dénomination française. Aussi, dans les descriptions qui suivent, pour les établissements qui seraient dotés d'un serveur d'identité, nous remplacerons « système GAM/GAP » par « serveur d'identités ».

La méthode de base de cette interface est de rendre la gestion patients du logiciel de GDR esclave du système de référence GAM/GAP. Toute information d'identité patient figurant dans la GDR provient exclusivement et directement de la GAM/GAP (même si, pour des raisons purement techniques, il y a réplication des données d'identité de la GAM/GAP dans la base physique des identités du logiciel de GDR). Dans ce cas le « dialogue identité patient» GDR - GAM/GAP est unidirectionnel, de la GAM/ GAP vers la GDR. Du point de vue fonctionnel, l'utilisateur qui aurait besoin de créer/ modifier l'identité d'un patient lors de la « prise de rendez-vous », sera contraint de le faire d'abord dans le logiciel GAM/GAP, puis de revenir dans le logiciel de GDR pour terminer son action initiale (prendre rendez-vous pour tel patient). On notera la criticité du délai de synchronisation de l'identité de référence GAM/GAP vers le logiciel GDR, avec les enjeux techniques et organisationnels qui peuvent en découler. Cette dualité n'aura pas d'incidence sur les utilisateurs qui n'ont pas d'habilitation à créer/modifier des identités, car les patients pour lesquels ils ont à prendre des rendez-vous sont censés être déjà connus, voire admis dans l'établissement (par exemple, les personnels d'unités de soins demandant des rendez-vous pour des patients hospitalisés).

Une méthode plus élaborée consiste maintenir l'accès utilisateur aux fonctionnalités de gestion des identités patients dans le logiciel GDR. Le système GAM/GAP peut conserver ses prérogatives d'arbitrage de référence en refusant les demandes de création/modifications d'identités qu'il estimerait non conformes. On notera, aussi dans cette configuration, la criticité des délais de synchronisation avec les mêmes enjeux techniques et organisationnels, car le dialogue entre les applications, s'il est bidirectionnel, met en œuvre la même famille de messages. L'avantage de cette méthode est que l'utilisateur du système de GDR reste dans son environnement métier GDR. La contrainte est que les règles de gestion des identités du GDR doivent être congruentes avec celles du système référentiel GAM/GAP pour limiter les rejets de demandes de création/modification pour non-conformité.

Une alternative consiste à supprimer au système de référence GAM/GAP sa mission d'arbitrage des conformités. Il faudra alors être vigilant en ce qui concerne l'aptitude du

système de gestion du GDR à mettre en œuvre ces règles pour maîtriser le risque de « pollution » du référentiel d'identité GAM/GAP par le système « connexe » GDR (connexe, du point de vue identification patient). Dans une telle situation, pourra-t-on encore considérer le système GAM/GAP comme le système référentiel de gestion des identités?

La criticité des délais de synchronisation

La « bonne » identité du patient est un préalable à la prise de rendez-vous et à la mobilisation d'une ressource pour lui réaliser un acte. Pas d'identité patient correcte, pas de prise de rendez-vous correcte. Dans l'architecture nécessairement bipolaire de la gestion de ces identités, les délais d'acheminement et de traitements des messages sont extrêmement critiques. Cette contrainte conditionne les choix d'architecture de communication inter-applications. Elle conditionne également la définition de procédures dégradées qui seront mises en œuvre lorsque la communication ne répondra pas normalement (*Une défaillance doit arriver !).* Ces procédures devront être conçues à différents niveaux de défaillances et d'acteurs impliqués, en fonction des choix techniques et organisationnels retenus (indisponibilité du système de référence GAMP/GAP ou indisponibilité de la connexion avec ce système, indis- ponibilité de « courte durée » ou de « longue durée », indisponibilité programmée ou non, réconciliation des données d'identité s'il est possible que le système GDR fonctionne temporairement en autonomie plus ou moins partielle…).

Les identités provisoires

La charte d'identitovigilance de l'établissement précise ce qu'est une identité provisoire *versus* une identité validée. Classiquement, une identité validée est une identité dont le recueil des caractéristiques – nom, prénom, date de naissance, etc. –, qu'on appelle « traits d'identité », a fait l'objet d'une confrontation avec, d'une part des documents d'identité de référence (carte d'identité, passeport, carte de séjour), d'autre part la présence physique du patient. Une identité est classiquement qualifiée provisoire dans toute situation de recueil réalisé par téléphone et/ou en l'absence de documents officiels d'identité en présence du patient. C'est par conséquent une situation fréquente, voire systématique, dans nombre de cas de prises de rendez-vous. Les identités des patients inconnus, totalement ou partiellement (l'orthographe du nom n'est pas attestée, le prénom pas sûr, la date de naissance incertaine), sont à traiter comme des identités provisoires.

Ces identités provisoires sont des identités à haut risque. Il faut absolument que le système de GDR les repère sans ambiguïté pour l'utilisateur. Cela permet, lors du contact avec le patient, de lui demander les informations et les documents nécessaires à la validation de son identité jusque-là provisoire.

Il existe deux grands modes de gestion des identités provisoires d'une architecture multipolaire vis-à-vis du système référentiel GAM/GAP.

Le plus courant consiste à traiter les identités provisoires localement dans chaque application, dont la GDR, et à ne « consolider » au niveau du système référentiel GAM/ GAP que les identités validées.

Un mode moins courant consiste à intégrer dans le système référentiel GAM/GAP la gestion de l'ensemble des identités provisoires.

Dans les deux modes, l'enjeu est la qualité de la consolidation d'une ou plusieurs identités

provisoires avec leur identité validée dans les différents systèmes concernés, notamment dans celui de la GDR. Cette consolidation peut donner lieu à la réconciliation d'une ou plusieurs identités provisoires dans la GDR avec l'identité validée du système référentiel GAM/GAP ou serveur d'identités.

Synchronisation de la fonction « gestion des patients » de la solution de gestion des rendez-vous et de planification des ressources à la gestion des patients

Dans ce cas, la solution de gestion des rendez-vous et de planification des ressources utilise sa propre gestion de patients, qui consiste en une réplique pure et simple de la gestion « générique » patient (à l'exception des patients « temporaires », *voir plus loin*). L'intégration est à sens unique, autrement dit elle permet uniquement un flux sortant pour la gestion patient et entrant pour la solution de gestion des rendez-vous et de planification des ressources. La solution de gestion des rendez-vous et de planification des ressources est un « esclave » du système maître (gestion patient). Il faut alors s'assurer que même si la connexion avec la gestion « générique » des patients est indisponible, les changements intervenus dans la gestion « générique » des patients resteront dans une file d'attente de messages qui sera traitée dès le rétablissement de la connexion. L'ensemble de la synchronisation peut s'effectuer au moyen de messages HL7 via une connexion TCP/IP ou une file d'attente de messages (MSMQ). Si les systèmes ne sont pas compatibles HL7 ou utilisent encore une syn- chronisation basée sur des fichiers, il faut que la solution de gestion de rendez-vous et de planification des ressources dispose de son propre outil de liaison de messages. Si aucune synchronisation HL7 ou basée sur des fichiers n'est prévue, idéalement, un moteur d'intégration tiers peut être utilisé pour effectuer la liaison et le routage. Si des messages ADT (relatifs à l'enregistrement des patients et d'épisodes) peuvent être transmis, ils pourront également être affichés dans la solution de gestion de rendez-vous et de planification des ressources.

Souvent, il est nécessaire de réserver un rendez-vous pour un patient inconnu dans la base patient. Dans ce cas, la secrétaire doit avoir la possibilité d'enregistrer un nouveau patient dans la solution de gestion de rendez-vous et de planification des ressources. En outre, il doit être possible de repérer le rendez-vous correspondant pour signaler que le patient n'est pas validé (patient « temporaire »). Le rendez-vous réservé avec l'identité « temporaire » devra être remplacé par l'identité « validée » (voir Messages d'épisode HL7). Comme pour les patients et les admissions, la solution de gestion de rendez-vous et de planification des ressources est le système esclave des épisodes. La solution de gestion de rendez-vous et de planification des ressources peut recevoir les informations d'épisode de manière à pouvoir associer des rendez-vous à des épisodes.

Le serveur d'identités unique (SIU) à plusieurs établissements et le rapprochement d'identités

Le serveur d'identification et de rapprochement permet aux établissements :

- la recherche d'identités,
- le rapprochement d'identités.

Son rôle est de fiabiliser l'identification des patients dans les SI et lors des échanges. Une identité d'un patient appartenant à un GHT est composée:

- de son domaine d'identification (ex : Finess),

- des traits la constituant,
- d'un état (validée).

Les règles de saisie des traits doivent obéir à une charte. Les standards associés sont:

- profils « identité » IHE,
- PAM: diffusion d'identités et de mouvements,
- PIX : rapprochement entre identités,
- PDQ: recherche d'identités.

Le serveur d'identités commun doit assurer l'unicité de l'identité des patients au sein du GHT. En fonction de l'organisation souhaitée par les établissements, les mouvements doivent pouvoir être réalisés de façon mono ou bidirectionnelle entre le dossier patient et les GAM.

Afin de faciliter la phase d'initialisation de la base d'identité commune (SIC), il faut donc s'appuyer sur un serveur de rapprochement. Chaque établissement identifie localement le patient dans son domaine d'identification avec son IPP local. C'est uniquement au niveau de l'environnement de coopération que les identifiants locaux des différents domaines d'identification seront rapprochés.

Le rapprochement est alors effectué par un traitement de rapprochement automa- tique sur la base d'un algorithme de rapprochement s'appuyant sur certains critères paramétrables avec un poids affecté en regard. Cet algorithme de rapprochement doit s'appuyer sur les traits d'identité du patient. L'algorithme de rapprochement doit aussi prendre en compte les cas où seulement une partie des critères est vérifiée. Les données de rapprochement (auteur, poids, critère retenu…) doivent être horodatées et historisées.

Terminologie

- Collision : dans un même domaine d'identification, un même identifiant est attribué à deux personnes physiques différentes.
- Domaine d'identification : regroupe au sein d'une organisation de santé toutes les applications utilisant le même identifiant pour désigner un patient.
- Domaine de rapprochement : on distingue les domaines de rapprochements intra et extra-établissement.
  - Défusion: action de dissocier un identifiant en deux identifiants.
- Doublon: dans un même domaine d'identification, une même personne physique possède au moins deux identifiants.
- Fusion : action de transférer sur un identifiant unique toutes les informations relatives à une personne physique et dispersées sur un ou plusieurs doublons.
  - IPP : identifiant permanent patient.
  - IEP : identifiant d'épisode patient.
  - INS-C : identifiant national de santé calculé.
  - INSEE : Institut national de la statistique et des études économiques.
- Identifiant: séquence de caractères utilisée par un ou plusieurs systèmes d'information

pour représenter une personne physique du monde réel.

- Identification du patient: opération consistant à attribuer de manière univoque à une personne physique un nouvel identifiant ou à retrouver un identifiant existant.
- Identification primaire : encore appelée « identification initiale », elle consiste à créer une identité dans le SIH ,et certains logiciels périphériques qui peuvent posséder un domaine d'identification particulier, ou à attribuer une identité connue à un patient.
- Identification secondaire : vérification par tout professionnel de santé de l'identité du patient avant la réalisation d'un acte le concernant (prélèvement, soins, transport). L'identification secondaire comprend également l'identification des prélèvements ou des documents du patient, ainsi que la sélection du patient dans une application périphérique au SIH (prescription connectée, dossier médical…).
- Identité : ensemble de données qui constitue la représentation d'une personne physique. Elle est composée d'un profil de traits. Pour l'identification primaire du patient dans les systèmes informatiques, l'identité est associée à un identifiant.
- NIR : numéro d'inscription au répertoire (NIR). Identifiant unique des individus inscrits au Répertoire national d'identification des personnes physiques (RNIPP) géré par l'Insee. Composé de treize caractères, ce numéro indique successivement et exclusivement le sexe (1 chiffre), l'année de naissance (2 chiffres), le mois de naissance (2 chiffres) et le lieu de naissance (5 chiffres ou caractères) de la personne concernée. Les trois chiffres suivants permettent de distinguer les personnes nées au même lieu à la même période.
- Traits : éléments d'informations propres à un patient, d'importance variable.
  - Ils sont dits « stricts » dès qu'ils permettent l'identification du patient. Les traits stricts contribuent au rapprochement automatique d'identités. Ces traits sont le nom de naissance, le prénom, la date de naissance, le sexe, le pays de naissance pour les patients nés à l'étranger et le lieu de naissance pour les patients nés en France (métropolitaine, DOM, TOM, POM).
  - Ce sont des éléments stables, vérifiables à partir de documents officiels comportant impérativement une photographie à l'exception du livret de famille pour les enfants mineurs ne disposant pas de carte d'identité.
  - Ils sont dits « étendus » lorsqu'ils apportent un supplément d'identification et permettent d'affiner l'identité de la personne (ex : nom usuel, adresse…). Ces elements ne sont pas stables dans le temps.
  - Ils sont dits « complémentaires » quand ils apportent des informations de type métier ou socioprofessionnel (ex : numéro de sécurité sociale, profession ou numéro de téléphone). Ils peuvent permettre d'affiner une recherche sur l'identité d'un patient.