GHT : le casse-tête de la gestion des identités vu par nos experts

Pour le DSI, l'IAM en ligne de mire

Le GHT est une fusion déguisée et, le temps de la convergence des SI, il va bien falloir déterminer des trajectoires sur chaque domaine fonctionnel. Évidemment, il faudra aller vers une DRH unique, qui utilise un progiciel RH unique pour gérer l'ensemble des agents de la superstructure issue de la fusion des n établissements du GHT. Mais avant cela, quelle trajectoire, quels besoins, quelles priorités ? Et surtout, dans l'objectif de déployer l'IAM[1], car l'annuaire des agents est une brique indispensable au futur SI du GHT.

Le besoin avant tout

Il est utile de revenir aux fondamentaux de l'expression des besoins, par exemple dans le contexte d'un établissement périphérique (P) qui souhaite mutualiser son processus RH avec l'établissement support (S).

La première étape consiste à uniformiser les règles de gestion RH : calcul des heures, des temps de repos, des primes, etc., autant de règles spécifiques à chaque établissement et pour lesquelles les discussions entre la direction et les instances représentatives du personnel (IRP) pourront durer des mois, voire davantage. Cette étape est de loin la plus politiquement compliquée tout en étant indispensable.

La deuxième étape pourra concerner le transfert vers S des fonctions RH sans véritable valeur ajoutée de P : hébergement technique du serveur RH de P (qui ne nécessite pas d'agrément HDS puisqu'il ne s'agit pas de données médicales), prise en charge du processus de paye (calcul, mise sous enveloppe des bulletins, transfert à la Trésorerie des fichiers de mandatement).

La troisième étape consiste en un transfert des fonctions RH de P vers S, sur le mode maîtrise d'ouvrage/maîtrise d'œuvre (MOA/MOE) : l'ordonnateur ou

responsable du traitement reste P, qui délègue le traitement RH vers S (qui est donc MOE du processus et agit sur ordre de P). Beaucoup d'entreprises privées procèdent ainsi, ce qui ne représente pas de difficultés techniques ou juridiques particulières si le transfert est correctement bordé : contrat, limites de responsabilité des acteurs, respect de la réglementation Informatique et Libertés dans l'optique du règlement général sur la protection des données (RGPD) de mai 2018, etc. La principale difficulté réside dans le fait que les agents de S vont devoir accéder à un autre progiciel RH que celui de S pour gérer les agents de P : d'où la nécessité de formations, de maintenance dudit progiciel, de suivi réglementaire, de montées de version, etc. Clairement, à ce stade, aucune économie d'échelle n'est réalisée : ce n'est pas le déplacement d'une fonction support d'un point A à un point B qui permet de réaliser des gains.

La quatrième étape porte sur la prise en charge totale de la fonction RH de P par S : recrutement, politique de formation, budgets RH, etc. À ce stade, en dehors des questions juridiques, une des problématiques majeures réside dans le fait que les agents de S vont utiliser un seul progiciel (celui de S) pour gérer à la fois les agents de S et ceux de P. Faut-il deux instances de bases de données, ou une seule mais avec une séparation logique ? Le progiciel RH permet-il une séparation logique et efficace ? Pas certain que cela soit possible, surtout dans un contexte de certification des comptes qui en demande toujours plus sur la séparation des rôles et les preuves techniques (traces) relatives au processus RH. C'est, clairement, une étape préalable à la fusion des processus RH – et les juristes diront si elle est ou non dissociable de la fusion des entités juridiques.

Le noyau avant le reste

Il serait faux de croire que la prise en charge RH se résume, sur le plan informatique, au transfert de responsabilité concernant un seul progiciel : le macro-processus RH est couvert par plusieurs logiciels, allant bien entendu de la paye et de la gestion des carrières à la médecine du travail (très sensible), en passant par la gestion des temps (gros travail d'uniformisation des règles entre P et S), des indemnités, etc. Dans un monde parfait, il faut commencer par transférer MOA et MOE sur le noyau (annuaire agent, paie et carrière), puis on peut attaquer les modules périphériques. Et comme, bien entendu, tout ne peut pas être fait d'un coup, une phase plus ou moins longue de transition est à prévoir.

Suite de l'article p. 26

[1] *Identity Access Management*

GHT : le casse-tête de la gestion des identités vu par nos experts (suite)

Vers l'IAM

Les établissements qui se sont engagés dans des projets de déploiement de cartes à puces multiservices (IAM) savent que l'informatisation de la fonction RH ne s'arrête pas là. Elle est intimement liée au provisionnement d'un méta-annuaire technique central utilisé pour alimenter les différentes sources : accès physique aux locaux, accès parking, accès SIH, accès self. Et surtout pour automatiser au maximum le provisionnement des habilitations applicatives, ce qui nécessite là aussi de dérouler des règles de gestion communes, et donc partagées par tous les acteurs : commission médicale d'établissement pour l'accès au dossier patient informatisé et aux fonctions supports (laboratoires, imagerie, pharmacie), DSI pour les fonctions bureautiques de base (messageries, partages de fichiers), etc.

La difficulté d'un tel projet provient aussi du fait que les sources des identités ne sont pas seulement issues des personnels payés par l'établissement, mais multiples : étudiants, stagiaires non rémunérés, personnels mis à disposition, internes, etc. La trajectoire d'un projet IAM est un véritable chemin de croix si cette dimension n'est pas prévue « by design » dans la refonte des processus RH du GHT.

Le point de vue du DSI met en évidence la nécessité d'organiser la coresponsabilité de traitement entre les membres du GHT. Mise en place à des fins cosmétiques, elle aboutirait vraisemblablement à une désorganisation importante, source de risques opérationnels et juridiques.
Pierre Desmarais

Ce qu'il faut retenir

L'IAM est une des briques de base du SI : ne pas l'avoir déployée, c'est se trouver de fait dans l'incapacité de faire face à certains besoins fonctionnels (délivrer les comptes et les habilitations aux utilisateurs en temps et en heure) ou aux contraintes exogènes (authentification forte de plus en plus exigée par les normes et les référentiels). La gestion des identités des agents au sein d'un GHT est bien entendu une question qui impacte le fonctionnement des DRH, mais se limiter à cette dimension revient à se contraindre de rejouer le film douloureux d'un projet IAM, à l'échelon d'un GHT. La liberté d'il y a quelques années de ne pas s'engager dans un projet IAM a disparu : les diverses certifications qui pèsent maintenant sur les établissements (certification des comptes, mais aussi Haute Autorité de santé) réduisent la marge de manœuvre à la portion congrue, et ne pas l'anticiper revient à s'introduire un énorme caillou dans la chaussure informatique.

La question que doivent se poser les DRH n'est donc surtout pas « comment mutualiser les fonctions RH au sein d'un GHT », mais bien « comment gérer les identités des agents ayant un lien contractuel avec tout ou partie des membres d'un GHT », ce qui est très différent.

Cédric Cartau

Pour le juriste, le début d'un casse-tête

La loi Touraine a introduit dans le Code de la santé publique un nouvel outil de coopération sanitaire : le groupement hospitalier de territoire. Ce que ne révèle pas expressément la loi, nous rappelle Pierre Desmarais, c'est l'identité du bénéficiaire de cet outil : l'État. En effet, le GHT poursuit manifestement un objectif de rationalisation de la gestion des établissements de santé publics et, de façon connexe, de réduction des dépenses de santé. Quoi de mieux alors, pour étrenner le système d'information convergent du GHT, que de commencer par quelque chose de simple, de standardisé, comme la gestion des ressources humaines ?

Problématique

Dans ce cadre se posera rapidement la question de la gestion de l'identité des personnels. C'est en effet la base. Sans elle, la gestion des ressources humaines est impossible et les droits d'accès au SI ne peuvent être accordés. Mais gérer l'identité des personnels passe par la mise en œuvre d'un traitement de données, lequel doit être mis en œuvre sous la responsabilité d'une personne physique ou morale. C'est le début d'un casse-tête que le législateur n'a pas souhaité résoudre.

Origine du casse-tête

Le GHT est une fusion d'établissements de santé publics qui cache son nom. Résultat, le GHT n'est pas une personne morale. Ce déguisement interdit la désignation du GHT en qualité de responsable de traitement, le droit français et européen ne permettant de faire peser des obligations que sur des êtres ou des entités disposant de la personnalité juridique. Il va donc falloir identifier un autre responsable de traitement que le GHT, solution qui aurait pourtant arrangé tous ses membres. Alors, qui, parmi les établissements membres et l'établissement support, détermine la finalité et les moyens du traitement nécessaire à la gestion de l'identité des personnels ?

Suite de l'article p. 28

GHT : le casse-tête de la gestion des identités vu par nos experts (fin)

Les membres du GHT pilotent-ils encore le traitement ?

Faute de fusion, chaque membre du GHT va rester l'employeur de son personnel. Les établissements continueront donc à définir individuellement la finalité de ce traitement de données. En revanche, ils perdront totalement la maîtrise des moyens du traitement, dès lors que la centralisation de la gestion de l'identité se fera au niveau de l'établissement pilote, lequel définira donc seul les outils nécessaires à la mise en œuvre de ce traitement.

L'établissement support ne pourra pas en endosser la responsabilité

Pour autant, l'établissement support ne pourra pas – et surtout, ne voudra pas – endosser la responsabilité de traitement. D'une part, parce que s'il ne maîtrise pas la totalité des ressources humaines des établissements, il ne peut assurer les obligations d'un responsable de traitement. D'autre part, faute de pouvoir imposer et contrôler le respect de ses directives par le personnel d'établissements juridiquement indépendants. De dernière part, en raison de la responsabilité juridique qu'il encourrait seul du fait du portage unilatéral de la responsabilité de traitement.

L'ébauche d'une solution

Le règlement général relatif à la protection des données, qui entrera en vigueur le 25 mai 2018, pourrait offrir l'ébauche d'une solution à ce challenge – et à tous ceux afférents aux traitements de données au sein du GHT – en permettant la mise en place de coresponsabilité de traitement. L'idée consisterait à ériger les établissements membres et l'établissement support en qualité de responsables et de répartir contractuellement – c'est alors une obligation autant qu'une nécessité – les rôles et les responsabilités de chacun. De la sorte, les membres pourront continuer à déterminer la finalité et à mettre en œuvre le traitement, tandis que l'établissement support pourra en définir les moyens. 2018 ? Mais le GHT, c'est maintenant ! Effectivement, mais la Cnil a appliqué le texte par anticipation dans une décision Facebook Inc. et Facebook Ireland du 27 avril 2017. Si la Cnil l'a fait, rien n'empêche les GHT d'en faire autant.

Mais une ébauche seulement

D'accord, nous avons désormais une solution pour mettre en place le traitement de données nécessaires à la gestion de l'identité des personnels, sans que l'établissement support se retrouve seul face à tant de responsabilités. Mais le casse-tête n'est pas résolu : on ne fait qu'en découvrir l'étendue.

Reste à savoir comment la confidentialité des données relatives aux personnels des membres est assurée. L'établissement support va-t-il opter pour la sécurité et créer une instance de base de données par membre ou se borner à créer des catégories spécifiques dans sa base pour chaque membre ? Dans le second cas, comment s'assurer que le personnel de l'établissement support n'interagira pas avec ces bases ? Comment éviter que les ressources humaines des membres ne consultent indûment les données relatives des autres membres ou de l'établissement support ? Le progiciel utilisé pour gérer l'identité des personnels permet-il de limiter les droits d'accès d'un utilisateur à une catégorie déterminée de personnels ? Comment gère-t-on la traçabilité, puisque l'établissement support verra l'identifiant des utilisateurs, sans connaître leur identité dans le SI des membres ? Des questions, encore des questions, et toujours sans vraies réponses.

La réponse viendra du terrain, mais pas du système D

Cet amas de questions n'étonnera pas le lecteur expérimenté. La pratique y répond habituellement par le système D. Mais avec des sanctions pouvant aller jusqu'à 4 % du chiffre d'affaires et une Cnil annonçant clairement son intention de « sensibiliser les personnes et les responsables de traitement aux droits et obligations issus de la loi Informatique et Libertés » par la sanction, ce n'est clairement pas la panacée. D'autant que rien ne garantit que les membres et l'établissement support auront le même seuil d'acceptabilité du risque juridico-financier. La réponse est donc ailleurs. Gageons que seul le terrain permettra de la trouver.

Pierre Desmarais

L'approche de la question sous l'angle du responsable du traitement rejoint la question du transfert de responsabilité MOA/MOE du point de vue SI. Que les deux visions se rejoignent démontre que nous ne devons pas, ni Pierre Desmarais, ni moi-même, être à côté de la plaque !
Cédric Cartau