Spécifications du système d'information hospitalier dans le cadre de regroupement d'établissements

Véronique Deslandres[*] — Ahmed Bounekkar[**]

** Université Lyon 1, laboratoire LIESP*

*** Université Lyon 1, laboratoire LIRIS*
Campus La Doua, F-691622 Villeurbanne cedex

RÉSUMÉ. *Cet article traite des modifications qu'entraîne le regroupement d'établissements hospitaliers sur le nouveau système d'information hospitalier. Le regroupement hospitalier concerne surtout le plateau médico-technique (PMT), c'est-à-dire l'ensemble du bloc opératoire et les services périphériques permettant de réaliser des investigations, des diagnostics et les traitements à l'aide de matériels coûteux et sophistiqués. Aujourd'hui les différentes entités qui composent le PMT gèrent leurs flux de manière indépendante et de nombreuses re-saisies sont nécessaires lorsqu'un patient circule d'un service à l'autre. La mise en place d'un nouveau système d'information requiert une démarche d'analyse et de spécifications mettant en œuvre des compétences relevant à la fois de management et de technologies de pointe. Nous abordons aussi bien les éléments de conduite de projet que les aspects techniques propres aux établissements hospitaliers. Les propositions ont été construites à partir d'accompagnements effectués par les auteurs auprès de différents partenaires hospitaliers concernés par la problématique du regroupement.*

ABSTRACT. *This paper studies the modifications which involves the gathering of hospitals on the new hospital information system. The hospital gathering relates to the medico-technical platform, the whole of the operating theatre suite and the peripheral services making allows to carry out investigations, diagnoses and the treatments using expensive and sophisticated materials. This paper takes into account especially the information system of the medico-technical platform. Actually the various entities which make the medico-technical platform workflow in an independent way and many repetitions of data recording are frequently necessary when a patient is transferred from one service to another. Implementing a new information system requires competences in project management as well as technical knowledge in advanced technologies. In this paper, those two aspects are studied in the specific context of hospital care. The proposals were built starting from accompaniments carried out by the authors near various hospital partners concerned with the problem of grouping together technical platforms.*

Mots-clés : système d'information hospitalier, sécurité, architecture des systèmes d'information, regroupement de plateaux techniques

Keywords: hospital information system, security, information system architecture, grouping together technical platforms

SAS – 10/2007. Systèmes d'information et santé, pages 65 à 81

1. Problématique du regroupement hospitalier

Le regroupement hospitalier est une problématique récente pour les établissements hospitaliers, qui sont maintenant soumis à de nouvelles obligations de rentabilité économiques. Le regroupement peut concerner le rapprochement de différents centres géographiquement distincts mais le plus souvent ce sont les plateaux médico-techniques (PMT) de différentes disciplines d'un même établissement qui doivent être regroupés au sein d'un pôle commun de services et de ressources. Le PMT est traditionnellement constitué des salles d'interventions chirurgicales et salles de réveil, des services de soins critiques, du service d'imagerie médicale, des salles d'explorations fonctionnelles et de l'ambulatoire.

Le regroupement des plateaux médico-techniques implique une réflexion sur le remaniement ou l'adaptation du système d'information (SI) de l'établissement de santé. C'est aussi l'occasion pour l'établissement de moderniser son système d'information global (SIH, système d'information hospitalier), et de préciser les relations de dépendances entre le SI du PMT et le SIH. Les systèmes d'information contribuent à optimiser les processus pour atteindre les objectifs du centre hospitalier. En effet, dans un établissement hospitalier, les décideurs souhaitent disposer d'indicateurs d'activité médicale afin d'orienter leur stratégie. De plus, l'activité de soins génère un grand nombre d'informations de natures diverses. La gestion et la communication de ces données par le personnel médical ou infirmier s'avèrent de plus en plus complexes. Les données médicales proprement dites sont étroitement liées aux informations médico-administratives. L'alignement stratégique du SI consiste à faire en sorte que le système d'information soit un atout au service de la stratégie de l'entreprise et qu'il fournisse aux professionnels les outils permettant de la mettre en œuvre (Henderson et Venkatraman, 1993).

Les différentes préconisations techniques qui suivent ont pour but de servir d'éléments de références dans la définition du besoin d'un établissement de santé dans un projet de modernisation de son système d'information et du SI associé au plateau médico-technique en particulier. Les préconisations sont cohérentes avec le référentiel de « bonnes pratiques » des systèmes d'information hospitaliers, présenté par le Groupement pour la modernisation du système d'information hospitalier (GMSIH, http://www.gmsih.fr). Le travail sur le système d'information avec des partenaires hospitaliers nous a amenés à plusieurs constats :

1. la demande est extrêmement forte d'améliorer et de reconsidérer certains aspects des systèmes d'informations de l'établissement : d'une part par des contraintes externes (T2A, CCAM…), mais également du fait des besoins internes et transversaux d'un pôle clinique à l'autre ;

2. le SI lié au PMT, ce dernier étant le cœur du métier d'un centre hospitalier, est fortement connecté au SIH et on ne peut pas faire l'économie de considérations générales (sécurité, architecture…) qui se répercutent au niveau du SI du PMT.

L'objectif du présent article est donc de proposer une méthode de travail pour aider les centres hospitaliers dans :

– la proposition d'une démarche de gestion de projet pour la spécification du SI du PMT (étapes, enjeux et risques, conditions de réussite, scénarios possibles) ;

– la spécification des besoins technologiques à partir d'informations à la fois prospectives sur le métier (identification des flux d'information futurs, compte tenu des contraintes juridiques ou liées à l'accréditation) et technologiques (architecture, stockage, sécurité, etc.).

2. Démarche de spécifications du SIH

L'objectif d'un système d'information hospitalier est d'optimiser la prise en charge de l'activité de soins en améliorant la gestion de l'information à l'intérieur du plateau médico-technique et d'améliorer la coordination des tâches médicales, administratives et logistiques effectuées au sein de l'établissement hospitalier.

Le plateau médico-technique comprend des secteurs pour lesquels l'informatisation est déjà bien poussée, c'est le cas de l'imagerie médicale qui est de plus en plus numérisée. Néanmoins, tout ce qui concerne la gestion d'éléments communs a été peu anticipée et reste donc dupliquée d'un secteur à l'autre : c'est le cas de la gestion des prescriptions, du dossier patient, des rendez-vous, du circuit médicament, du serveur de demandes et de résultats.

On trouvera en figure 1 un exemple de passerelle entre le SIH et le PMT, où l'on voit les échanges d'informations opérés pour une succession d'examens différents. On constate que le dossier patient et les actes sont au cœur des échanges.

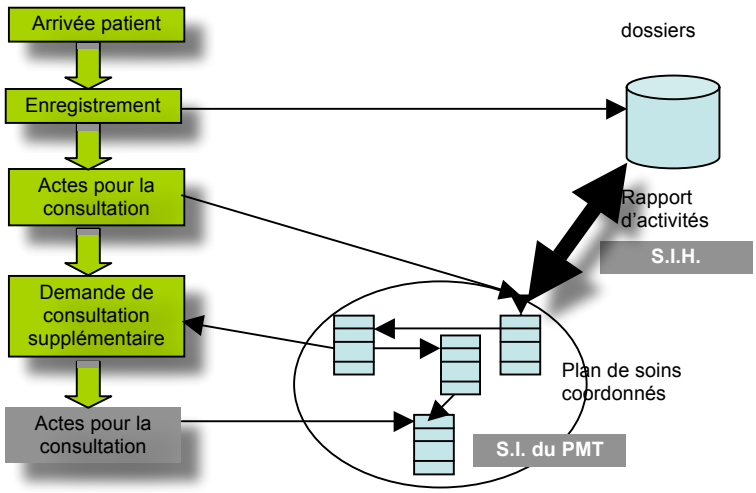

Figure 1. *Processus patient : liens SI du PMT et SIH*

2.1. *Les causes du retard*

Les établissements de santé accusent un retard important en termes de SI, qui devrait néanmoins s'atténuer avec la prise de conscience récente de ce retard et des difficultés que cela engendre. Les causes de ce retard ont été largement analysées (Fieschi 2003, Thibault, 2005), citons notamment :

– une offre logicielle insatisfaisante : marché de petite taille et peu lisible aux non spécialistes, ce n'est que depuis 2005 que quelques acteurs (étrangers) investissent le marché français et proposent des solutions centrées sur le cœur de métier de l'hôpital (la production de soins), persistance d'une double offre publique/privée dans un contexte de concurrence ambiguë, encore peu d'échanges standardisés ;

– une mauvaise perception de la dimension « système d'information » : le SI correspond trop souvent à un « outil » purement technique qui n'implique que peu de considération préalable pour son établissement ou lors de son évolution dans les services. Cela se traduit aussi par une faiblesse du budget consacré aux systèmes d'information, qui stagne à 1,5 % alors qu'il est de 30 % en moyenne dans les pays européens. Depuis sa création, le GMSIH essaie d'instaurer une nouvelle vision du SI et propose tout un panel de méthodes et d'outils, ainsi que des démarches de conduite du changement, adaptées au contexte des établissements de santé ;

– difficultés managériales : manque d'expérience et de compétences au sein des établissements en termes de gestion de projet face aux projets de SI qui sont complexes en milieu médical compte tenu des aspects sécurité, obligations légales, pluridisciplinarité des acteurs impliqués et diversité des interrelations à traiter ; absence d'une véritable démarche d'accompagnement du changement ;

– un historique en matière de gestion des SI lourd de conséquences : les établissements hospitaliers ont eu tendance jusqu'à présent à répondre au coup par coup pour concevoir leurs SI ; cela se traduit par un patchwork d'applications très diverses (plutôt orientées métiers) non connectées les unes avec les autres. Or ce type de système d'information, peu souple par construction, s'avère au fil du temps de plus en plus lourd et est coûteux à faire évoluer ;

– une grande variété d'acteurs impliqués dans les projets de SI : personnels de la Direction (DG, DSIO), leaders médicaux, personnel administratif (secrétaires médicales et soignants) qui rendent difficile l'adhésion de l'ensemble des personnes impactées par les systèmes d'information ;

– difficultés techniques : elles sont liées principalement à l'intégration et à l'absence d'architecture cible. Par ailleurs, certaines fonctionnalités sont « difficiles » à positionner dans l'urbanisation du SI de production de soins puisqu'elles relèvent de plusieurs pôles d'activité. Il s'agit de la gestion des RDV, de l'utilisation des serveurs de résultats, de la prescription de médicaments. Une autre difficulté plus récente est liée à l'utilisation croissante de postes de travail nomades, dédiés essentiellement aux fonctions les moins bien informatisées jusqu'à présent, la gestion médicale.

Nous avons constaté que le projet de regroupement motive fortement les centres hospitaliers à optimiser le système d'information utilisé au niveau du PMT. Certains auteurs fournissent des recommandations pour les spécifications d'un SIH à l'attention des centres hospitaliers (GMSIH 2005, Romeyer et Fabbe-Costes, 2004). Ayant accompagné différents centres dans leur projet de regroupement, nous suggérons que les phases du projet de spécifications du SI dans un centre hospitalier, et du SI du PMT en particulier, se déroulent de la manière suivante :

1) expression de besoins et refonte des processus,

2) élaboration de cahiers des charges détaillés,

3) conduite et négociation d'appels d'offres,

4) aide à la sélection des outils et des prestataires,

5) recette,

6) déploiement et conduite du changement.

2.2. *Les différentes phases dans un contexte hospitalier*

Tout projet de système d'information suppose l'implication de deux acteurs principaux, la maîtrise d'ouvrage (MOA) et la maîtrise d'œuvre (MOE). Le centre hospitalier (CH) dans son rôle de maître d'ouvrage doit être un véritable « acteur » dès le début du projet (trop souvent, on observe une certaine passivité qui peut être néfaste à terme). Nous proposons dans cette section d'étudier les phases les plus significatives du contexte hospitalier avec des illustrations de situations observées avec nos partenaires.

2.2.1. *Expression de besoins, refonte des processus et cahier des charges fonctionnel*

Il s'agit d'abord de dresser un état des lieux permettant l'identification des informations et des systèmes actuellement utilisés. Cet état des lieux peut s'effectuer à l'aide d'une analyse des processus, exploitant par exemple les résultats d'une accréditation effectuée antérieurement. L'état des lieux est suivi d'une refonte des processus, consistant à définir les fonctionnalités attendues du futur système.

Cette première étape est délicate et conditionne fortement le succès du projet. Tous les représentants des utilisateurs finaux doivent être impliqués dès cette phase, c'est une sorte de garantie d'une bonne acceptation du changement que va entraîner le nouveau système. Cette phase est effectuée sous la responsabilité du maître d'ouvrage, assisté si possible d'un partenaire universitaire compétent, d'une assistance du GMSIH ou d'un cabinet de conseil. Le résultat est un document contractuel appelé « cahier des charges fonctionnel » auquel on ajoute les contraintes fonctionnelles (robustesse, temps de réponses, etc.) sur lequel MOA et MOE se mettent d'accord. Le CH ne doit théoriquement pas mentionner de choix technologiques du type « un ERP serait souhaité », c'est le rôle du MOE de définir la solution technologique la plus apte à répondre aux besoins exprimés.

2.2.2. *Etablissement du cahier des charges détaillé*

La MOE présente la meilleure solution technologique dans un cahier des charges détaillé auquel est parfois joint une maquette ou un prototype. Pour ce qui concerne le SI d'un PMT associé à une refonte globale du SIH, trois solutions d'intégration se présentent :

– soit l'établissement choisit d'intégrer les systèmes existants par une approche de briques intégrées avec un pool de données centralisées (datawarehouse et approche EAI, Enterprise Application Integration, ou environnement d'applications intégrées) ;

– soit il choisit l'approche totalement intégrée avec un progiciel de gestion intégré (PGI ou ERP santé) : cette solution est particulièrement adaptée au contexte mais la mise en œuvre peut demander du temps, voire de légères modifications des applications existantes ;

– soit il choisit d'utiliser un PGI pour certains domaines fonctionnels, qu'il intègre ensuite *via* un outil d'EAI (approche mixte).

La deuxième solution est généralement choisie par les établissements disposant de compétences technologiques insuffisantes et qui acceptent l'idée d'un gros projet (investissement en temps et en argent éventuellement important) ; les premiers et derniers choix requièrent une certaine maîtrise technologique (par ex. la présence d'un ingénieur clinicien). En effet la mise en œuvre de ces solutions repose généralement sur une architecture n-tiers avec un découpage en couches (présentation, application, stockage des données), chaque couche ne communiquant qu'avec la couche adjacente, et qui permet une souplesse d'exploitation et de maintenance. Ces aspects techniques sont détaillés dans la section 3.

2.2.3. *Conduite et négociation d'appels d'offres*

Ces derniers peuvent se dérouler en suivant une procédure de dialogue compétitif, conformément aux articles 36 et 67 du code des marchés publics. Un tel choix est en général motivé par la complexité du marché et du projet associé. Si la recherche d'un SI pour le PMT d'un établissement entre dans un cadre plus global de refonte du SIH, il peut s'avérer pertinent de lancer une telle procédure. Cette procédure permet, dans le respect de l'égalité de l'information donnée aux candidats, de pouvoir concevoir une solution technique apte à satisfaire les besoins exprimés tout en ayant pris en compte les contraintes, les risques et le SIH existant. Le dialogue est réalisé sur la base d'un programme fonctionnel ou d'un projet partiellement défini. Les discussions avec les candidats ont lieu jusqu'à ce que l'établissement soit en mesure d'identifier précisément la ou les solutions répondant le mieux à ses besoins et à sa cible. On arrête à ce moment-là le cahier des charges (il n'est donc précisément établi qu'à la fin du dialogue compétitif) et les candidats sont invités à remettre leur offre.

La négociation avec les fournisseurs de la future solution concernant le montage financier du dossier est délicate et capitale, dans la mesure où elle peut constituer un moyen pour l'établissement d'inciter les sociétés concernées à mettre en œuvre une solution qui correspond *in fine* aux attentes des utilisateurs retranscrites dans le cahier des charges.

Afin de se prémunir d'un éventuel désinvestissement en cours de projet de son fournisseur ou de choix fait par la société dans le cadre du projet qui ne lui conviendraient pas, le CH peut découper le projet en plusieurs tranches (analyse fonctionnelle ; paramétrage ; déploiement), une tranche n'étant déclenchée que lorsque l'établissement valide la précédente. Par exemple, le fournisseur de la solution doit fournir à la fin de la première tranche un document décrivant les scénarios fonctionnels de la solution proposée, prenant en compte l'ensemble des situations de travail des utilisateurs et définissant les charges de travail de paramétrage et de formation concernant le dossier patient. Si le CH n'accepte pas le contenu du document, il peut tout à fait ne pas mettre en œuvre la tranche suivante.

2.2.4. *Aide à la sélection des outils et des prestataires*

Pour le choix d'un PGI, il faut savoir qu'il existe deux types de progiciels : les PGI « standard » qui ont fait leurs preuves dans d'autres domaines applicatifs (industriels notamment : c'est le cas de SAP et Oracle), et les plus récents PGI dédiés Santé (Cerner, Siemens). A ce jour, ni SAP ni Oracle n'ont réussi de percée marquante dans le domaine de la santé en France. On notera cependant que la stratégie d'Oracle, qui s'appuie sur un noyau applicatif, est plus ambitieuse, mais également beaucoup plus risquée que celle de SAP, qui propose une solution intégrée plus traditionnelle. Les éditeurs de PGI issus directement du monde de la santé maîtrisent le domaine « métier » de l'hôpital et possèdent une stature internationale qui leur donne sans doute les moyens d'adapter au contexte français des solutions éprouvées par ailleurs.

Là encore, le GIMSIH propose un guide de meilleures pratiques concernant l'intégration d'un PGI dans un SIH (GIMSIH 2005), qui porte sur deux aspects : d'une part la gestion de projet (maîtrise d'ouvrage, maîtrise d'œuvre, fournisseurs de composants) ; et d'autre part, l'aspect contraintes (volet organisationnel, volet fonctionnel, volet technique et volet financier).

2.2.5. *Recette*

Encore appelée « essais de réception », la recette consiste à vérifier la conformité de l'ouvrage à la demande formulée dans le cahier des charges. La recette est un processus rigoureux et méthodologique effectué dès la réception de la commande (par ex., installation du PGI santé). Elle est réalisée conformément au dossier de contrôle établi par la maîtrise d'ouvrage, rassemblant les documents définissant comment l'ouvrage doit être contrôlé.

2.2.6. *Déploiement et conduite du changement*

Le déploiement consiste à généraliser le nouveau système auprès de l'ensemble des utilisateurs finaux. Même s'il a été testé sur des sites pilotes avec succès, le déploiement généralisé peut échouer. En effet, lors de l'expérimentation, les utilisateurs ont une motivation que les utilisateurs finaux n'ont pas. La généralisation implique généralement des changements dans la façon de travailler des utilisateurs, ce qui freine l'adoption du produit par les utilisateurs. La conduite du changement permet de faire en sorte que les utilisateurs finaux acceptent et utilisent réellement le produit. Ce terme englobe notamment la formation des utilisateurs à l'utilisation du produit ainsi que l'accompagnement des utilisateurs *(hot line)*.

Associée à l'implémentation du nouveau SI, une nouvelle organisation des services va être mise en place et doit donc être préparée pour faciliter son acceptation par le personnel qui va utiliser la technologie. Différents scénarios de mise en œuvre existent, et il s'agit d'arbitrer entre les risques pour choisir le scénario le plus approprié à son projet :

– changer l'organisation avant la mise en place du nouveau système ;

– introduire le nouveau système et changer l'organisation en même temps ;

– introduire le nouveau système puis changer l'organisation.

Le GMSIH observe que dans la fonction publique hospitalière, la tendance majoritaire est le scénario 3. Si cela semble demander moins de charge de travail, cela peut engendrer une multiplication des dysfonctionnements qui démotivent les utilisateurs. Notre propre expérience d'accompagnement d'organisations industrielles dans l'introduction d'outils informatiques centralisés (de type ERP) confirme l'idée que c'est un mauvais scénario qui conduit généralement à une mauvaise perception de l'outil, voire à son rejet. Avec les CH, nous avons observé les scénarios 1 et 3, le scénario 1 étant souvent associé à une démarche de projet globale à laquelle la Direction de l'établissement a fortement participé.

Comme souligné précédemment, la démarche de conduite du changement doit toutefois être instaurée bien avant la phase de déploiement, dès la définition des besoins en matière de SI. En outre, c'est aussi un effort continu car il y a un fort taux de rotation dans les hôpitaux : nouveaux internes, personnel intérimaire ; ce qui peut amener à prévoir d'organiser des séminaires mensuels de formation aux outils informatiques.

3. Aspects techniques du système d'information du plateau médico-technique

Dans cette section, nous abordons brièvement l'évolution des modèles de conception des systèmes d'information hospitaliers et ses différents composants. L'intérêt de l'interopérabilité dans une stratégie transversale est ensuite mis en

évidence. Le développement des nouvelles technologies de l'information, et la complexité des systèmes d'information hospitaliers rendent incontournable l'utilisation des architectures web. Nous spécifions notamment les besoins auxquels répond ce type d'architecture dans les centres hospitaliers. Enfin des préconisations en termes de sécurité sont proposées en fin de section.

3.1. *Evolution des architectures*

Globalement dans tous les pays, la conception du SIH a beaucoup évolué ces 20 dernières années, passant d'une vision verticale dédiée, où les systèmes répondaient à un service de soins spécifique (par ex. : urgences, radiologie, laboratoires), à une conception plus transversale avec des fonctionnalités centralisées (dont une gestion centralisée du dossier patient). Du temps des mainframes, les éditeurs français étaient peu présents au sein des premiers grands systèmes d'information hospitaliers, puis l'offre française s'est progressivement étoffée dans le milieu hospitalier sous la forme d'applications client-serveur verticales sectorielles, c'est-à-dire spécifiques à un service ou une unité de soins. Mais les progrès de la technologie informatique et l'émergence de standards internationaux remettent en cause cette architecture verticale des systèmes d'information et favorisent la mise en place d'une architecture à base de composants. S'inspirant de l'exemple industriel, les éditeurs du secteur santé se mettent alors à développer des composants applicatifs spécifiques fédérés par des composants d'intégration génériques. Dès le milieu des années 90, des projets européens ont soutenu la notion de couche middleware applicative pour faciliter l'intégration des SIH. L'architecture de référence *Health Information System Architecture* (HISA) proposée en 1997 comme norme européenne est ainsi organisée en trois couches : la couche applicative, le middleware d'intégration et la couche de stockage (Degoulet et Fagon, 2004). Ainsi tout système d'information clinique est constitué de quatre couches logicielles comme représenté sur la figure 2.

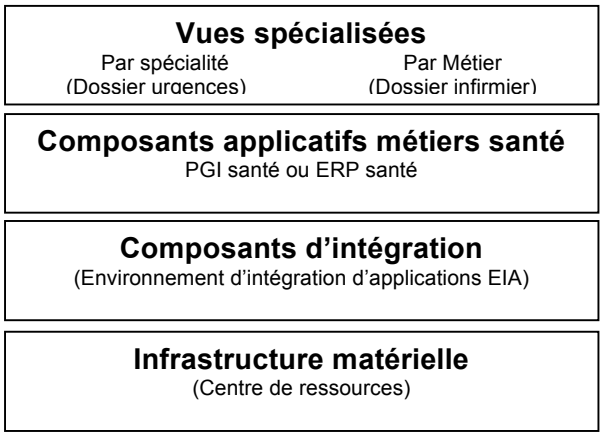

Figure 2. *Architecture en quatre couches (4-tiers) d'un système d'information hospitalier*

Les composants *de soins* nécessaires pour l'informatisation de la production de soins d'un hôpital (niveau 3 de la figure 2) sont au minimum :

– un composant de gestion des identités et des mouvements *(Patient Component* dans le modèle HISA) : ce composant trace l'activité mise en œuvre par l'équipe soignante pour répondre au problème du malade : information recueillie sur le patient, constitution et consultation du dossier du malade, connaissances médicales, processus de décision;

– un composant de gestion du dossier patient commun *(Healthcare Record*) : le dossier patient commun centralise les flux résultant des actions médicales : prescriptions, résultats, transferts, archivages. Ce composant assure la logistique entre les divers services cliniques et plateaux techniques de l'établissement pour appuyer l'activité de l'équipe soignante. Il permet d'effectuer a posteriori des études sur l'ensemble des dossiers, à des fins épidémiologiques ou d'évaluation de la qualité des soins, alimentant en retour la connaissance médicale ou l'administration. Différentes « vues » (filtres) du dossier patient permettent d'obtenir les dossiers métiers nécessaires aux différents acteurs (infirmiers, administratif, etc.).

– un composant de gestion des prescriptions et de suivi du workflow associé *(Activity Component*). Ce composant assure la gestion des actes médicaux et chirurgicaux, et peut également fournir une aide à la prescription médicamenteuse. L'analyse d'activité effectuée a posteriori fournit la vision stratégique nécessaire à une meilleure planification hospitalière, et permet d'engager des décisions d'investissement structurels, matériels et humains ; elle permet d'autre part d'alimenter les synthèses d'activités fournies aux entités extérieures (autorités de tutelle).

- un composant de gestion des ressources et des rendez-vous *(Ressource Component*) pour l'administration quotidienne de l'hôpital : facturation, gestion du personnel, gestion des stocks et comptabilité.

Ces quatre composants « de soins » ne sont pas indépendants et forment un progiciel de gestion intégré santé (ou ERP santé). D'autre part des composants génériques (niveau 2 des figures 2 et 3) s'ajoutent qui rendent possible le partage des informations et permettent l'intégration des composants dédiés aux soins. Ce sont notamment :

– le composant sécurité pour la gestion des utilisateurs et des droits d'accès (*Authorization Component* du modèle HISA). Les informations médicales et administratives des patients sont des données sensibles. L'accès à l'information doit

être contrôlé en fonction du profil de l'utilisateur. Le contrôle d'accès peut être réalisé selon différents procédés et/ou selon le type de dossier ;

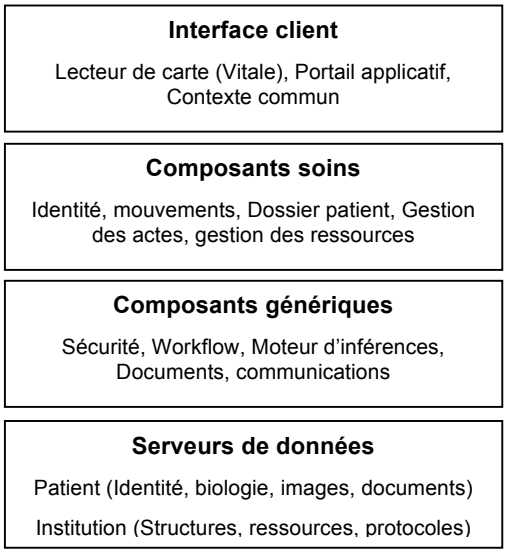

Figure 3. *Composants d'un SI hospitalier*

– le composant Référentiels *(Knowledge Component* du modèle HISA) : services et unités de soins, référentiels médicaux (diagnostics, actes, médicaments, etc.) ;

– un outil de workflow pour gérer l'enchaînement des fonctionnalités et les échanges de données ;

– un moteur d'inférences pour l'exécution des règles métiers (règles de bonne prescription, règles comptables, etc.) ;

– un gestionnaire de documents (indexation en particulier) ;

A ces différents composants s'ajoutent des outils intermédiaires pour la gestion des messages et l'encapsulation d'applications existantes (traducteurs et médiateurs).

Ces composants génériques constituent un environnement d'intégration d'applications (EAI), cela signifie qu'ils peuvent être réutilisés pour l'organisation et le pilotage de tout système applicatif, en intégrant les composants spécifiques dans une architecture globale.

3.2. *L'interopérabilité*

Par définition, l'interopérabilité d'un « service » (programme, application, fonction) est la caractéristique qui lui permet d'être accédé depuis des environnements différents de celui qui l'héberge. Cela suppose que le format de message, le mécanisme d'invocation de service et les mécanismes de sécurité soient compris par les consommateurs et le fournisseur du service. L'interopérabilité concerne trois champs d'investigation :

– l'échange de données entre différents équipements et systèmes d'information ;

– l'intégration de données hétérogènes pour des représentations multimédia ;

– la communication de telles données entre des services ou utilisateurs externes du secteur de la santé, de façon à faciliter la mise à disposition d'enregistrements électronique de santé.

La stratégie présentée précédemment par composants transversaux va dans le sens d'une meilleure interopérabilité par rapport à l'approche verticale de développements spécifiques aux différents secteurs, qui a prévalu ces 20 dernières années. Ainsi les ressaisies, redondance d'informations, demandes d'information d'un service à l'autre sont réduites à leur strict minimum. Un même composant peut être partagé dans tous les services d'un établissement ou dans les centres hospitaliers d'une région, par exemple pour l'identification des patients. Une meilleure sécurité peut être obtenue en définissant des protocoles d'accès et d'utilisation (les habilitations) entre les entités qui exploitent le composant. Il est également plus facile de maintenir et de former les utilisateurs en cas d'outils transversaux : les fonctions génériques (par ex. l'authentification) sont localisées et standardisées, et elles sont partagées par l'ensemble des composants dédiés.

L'interopérabilité est d'abord rendue possible par le dossier médical informatisé (DMI) du patient qui est le cœur du SIH. Chaque patient ayant un dossier unique, le DMI permet la gestion des patients hospitalisés comme des patients d'ambulatoire ou d'urgence. Il regroupe les données administratives, les informations cliniques (histoire du patient, allergies et intolérances médicamenteuses, examen physique, notes de suivi), les résultats biologiques, des images, des notes de transmission infirmières, des constantes vitales, des prescriptions -avec leur statut et les rendez-vous associés- ainsi que les résultats des examens. Ces informations sont stockées de avec l'heure et l'identifiant de celui qui saisit l'information, et rien ne peut être effacé.

3.3. *La technologie web*

La technologie web est un excellent support pour l'informatisation d'un centre hospitalier et de son réseau d'utilisateurs (postes nomades, consultations où actions à distance, etc.). L'architecture web a été choisie pour le SIH d'un centre hospitalier

partenaire du projet HRP2. La technologie choisie répond notamment aux besoins suivants, qui sont partagés par de nombreux établissements :

– les postes utilisateurs et les serveurs sont connectés à Internet ;

– les serveurs restent en interne, ils ne sont pas externalisés ;

– les postes utilisateurs sont des clients légers : dans un schéma d'architecture informatique de type clients-serveurs, Windows demeure incontournable comme système d'exploitation sur les serveurs pour héberger les applications telles que la facturation ou la comptabilité. La communication clients-serveurs se fait principalement avec un des deux protocoles suivants : Windows Terminal Services (TSE) ou Citrix, la deuxième solution étant très nettement plus onéreuse que la première.

– mise en place de serveurs web et d'un serveur de messagerie, ouverts sur l'extérieur ;

– logiciels (comptabilité, facturation, gestion de production) mis à jour à distance par les prestataires informatiques ;

– connexion d'ordinateurs non administrés par le service informatique sur le réseau informatique de l'établissement (postes des médecins notamment).

Pour une architecture web, on a le choix entre deux sortes de poste client. Avec le *client riche Internet*, le navigateur télécharge et exécute un ou plusieurs programmes qui dialoguent avec le serveur avec des messages XML. Grâce à la toute récente technologie AJAX, seules sont alors rafraîchies les zones du navigateur qui ont besoin de l'être et le confort d'utilisation est donc grandement amélioré. Néanmoins l'interconnexion de l'application avec le système ou les outils bureautiques reste difficile et ce type de client ne devrait subsister à terme que pour des sites web. Les entreprises préfèrent généralement déployer leurs applications avec un *client riche autonome*, pour lequel le navigateur ne sert qu'à télécharger et lancer une application qui fonctionne ensuite de façon quasi autonome. L'application s'exécute en effet dans un run-time tel que la plate-forme Microsoft .Net ou Java. L'utilisateur possède ainsi le confort d'un client lourd, avec un accès à toutes les fonctionnalités de l'application web et où les outils de bureautique restent accessibles. Dans ce cas, la contrainte porte donc sur la plateforme, qui doit être préalablement installée, de même qu'un moteur de chargement et de mise à jour automatique de l'application et du run-time ; l'administrateur se trouve par contre déchargé des tâches de déploiement et de mises à jour.

3.4. *La sécurité*

La protection des données concerne toutes les formes de l'information médicale, quelle soit écrite, orale ou électronique. L'article 29 de la loi du 6 janvier 1978 mentionne ainsi que l'établissement doit « prendre toutes précautions utiles afin de

préserver la sécurité des informations (nominatives) et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés ». Les standards de sécurité préconisés dans tous les pays concernent spécifiquement le dossier médical patient (EMR *Electronic Medical Record*) et couvrent toutes les entités médicales qui maintiennent ou transmettent des informations de santé électroniques. Au-delà des besoins habituels en sécurité et des solutions, technologies et techniques de sécurisation, connues et reconnues et même éprouvées dans d'autres secteurs d'activité, il faut constater que la « sécurité des systèmes d'information de santé » est un domaine plus sensible que dans d'autres secteurs puisqu'il cumule des exigences (le plus souvent fortes) sur les quatre axes de besoins :

– disponibilité,

– intégrité,

– confidentialité (politiques de management de la sécurité, politiques d'authentification forte, politiques d'autorisation fiables et de contrôles d'accès fidèles, voire politiques d'anonymisation et/ou de pseudonymisation, etc.)

– auditabilité avec des points de contrôles (placés *a priori* et pour prévenir les fraudes et irrégularités) et des éléments de preuve techniques (imputabilité) et/ou juridiques (opposabilité) pour garantir la correcte manipulation des informations et la licite utilisation des dossiers médicaux partagés.

L'objectif affiché du groupe sécurité de l'AFNOR est ainsi « d'apporter les éléments de confiance que la sécurité se doit de garantir dans un contexte aussi sensible que celui de la santé pour les systèmes d'information de santé. Ce groupe fournira des propositions pour des sujets essentiels pour « bâtir la confiance dans les systèmes d'information de santé ». Certains secteurs d'activités de la santé sont plus ou moins concernés par les aspects sécurité. La CNIS (Commission de normalisation des informations de santé de l'AFNOR) se penche par exemple sur l'opportunité d'un référentiel de sécurité pour la médecine ambulatoire. Un parallèle peut être effectué avec la démarche préconisée pour les dispositifs médicaux. Les contrôles effectués sur les équipements médicaux dépendent du risque évalué pour la sécurité du patient. L'approche qui a été choisie par les organismes de normalisation (USA, Canada et Europe) est d'affecter les équipements médicaux à différentes classes de risques. Plus le risque est élevé pour le patient et plus les contrôles sont rigoureux et poussés. Si l'instrument de mesure pour assurer la sécurité du patient des systèmes informatiques de santé peut de la même façon être rapporté au risque qu'ils peuvent présenter pour la santé du patient, alors les systèmes informatiques de santé devraient également être classés en fonction du risque (AFNOR, fév. 2006).

On observe donc que l'aspect sécurité des SIH est encore loin d'être abouti par les grands organismes de normalisation, et que les établissements sont dans leur grande majorité contraints de définir des règles et des pratiques propres leur permettant d'assurer un niveau minimal de sécurité.

Entre autres recommandations, on peut souligner que l'utilisation d'un portail d'accès sécurisé, avec signature unique des utilisateurs quelque soit les applications (Single Sign On), est un progrès réel. Ce type de portail ne doit toutefois pas être considéré comme une couche supplémentaire qui, une fois ajoutée à un ensemble d'applications verticales, pourrait être vendue comme la solution miracle aux limites d'interopérabilité. Un décret d'application récent (15 mai 2007) relatif à la confidentialité des données médicales à caractère personnel conservées sur support informatique ou transmises par voie électronique, précise que dorénavant l'accès à toutes les données personnelles des patients doit passer par l'authentification préalable d'une Carte Professionnelle de Santé. Cette carte personnelle lancée en 1993 concerne tous les professionnels de la santé et les personnels d'établissement. Elle devrait permettre au sein d'un établissement notamment de mieux contrôler l'accès aux données et de tracer les consultations/écritures du dossier patient.

Un autre aspect important de sécurité concerne le WIFI : les centres hospitaliers commencent à s'intéresser à cette technologie parce qu'elle permet la mobilité de l'utilisateur. Cela offre par exemple la perspective d'avoir un outil informatique lors des visites des patients par leur médecin, avec des supports de type PDA ou Tablet PC. Mais le WIFI peut présenter des risques en termes d'intrusions et la mise en place d'une solution WIFI doit être accompagnée par un professionnel installateur de réseaux sans fil sécurisés. Le coût d'une telle installation est très important et nécessite une étude de prix. La sécurité informatique demande une connaissance technique importante avec de fréquentes « mises à jour ». Sur ces aspects, la participation d'un prestataire de service est parfois incontournable. Néanmoins la direction de l'établissement a également un rôle à jouer : l'effort de sensibilisation de tous les personnels doit être décuplé dans les prochaines années afin que la culture en termes de sécurité des systèmes d'information gagne en maturité.

3.5. *Quelques aspects de sécurité traités par nos partenaires*

Au sein des établissements hospitaliers participant au projet HRP2, la quasi-totalité des postes informatiques est connectée à Internet. Cette situation demande une certaine vigilance face aux virus et aux intrusions. En conséquence, la sécurité doit être une priorité de la direction de l'établissement. La première nécessité est une protection à la tête du réseau interne, elle doit comporter un pare-feu *(Firewall)* qui ferme des ports de communications, un antivirus qui vérifie l'absence de virus dans les fichiers importés de l'extérieur et un proxy qui a une fonction de sécurité appelée « filtrage » interdisant l'accès à des sites internet à risques référencés sur des « listes noires ». Ensuite le parc informatique lui-même doit être sécurisé, les serveurs et les postes utilisateurs sont à protéger. Les serveurs *in situ* doivent avoir un antivirus local automatiquement maintenu à jour et les mises à jour de sécurité du système d'exploitation doivent aussi être automatisées. Les postes utilisateurs étant des clients légers, ils ne sont pas soumis à des risques directs, par contre ils peuvent être une

source de risques pour les serveurs. Les clients légers permettant aux utilisateurs de travailler à distance sur les serveurs, les droits utilisateurs devront être finement configurés pour qu'en aucun cas la stabilité du système et sa sécurité ne puissent être mis en danger. Si certains postes utilisateurs utilisent des applications locales, comme c'est le cas principalement pour les cadres de la direction qui utilisent des outils informatiques spécifiques ou la connexion à des périphériques (ex : PDA), le poste dispose alors d'un système d'exploitation complet, mais avec des droits utilisateurs restreints et un antivirus en local.

Un problème de sécurité peut également survenir via les postes « personnels » des médecins, qui se connectent (après autorisation) au réseau informatique du CH, ces postes ayant des droits « administrateur » sur la machine et n'étant pas 'contrôlés' par le service informatique. Le risque encouru est que la machine connectée peut alors propager les virus qu'elle possède. Pour éviter ce phénomène, on découpe le réseau physique en plusieurs réseaux locaux virtuels (VLAN). Les ordinateurs de deux VLAN ne pourront pas communiquer ensemble et par conséquent, le VLAN des serveurs et postes utilisateurs du CH ne pourra pas être contaminé par un ordinateur infecté présent sur un autre VLAN. Mettre en place des VLAN nécessite d'avoir des commutateurs qui permettent cette fonction. D'autres situations à risque peuvent apparaître : considérons à présent que le CH héberge un site internet ainsi qu'un serveur de messagerie. En d'autres termes, ces serveurs du CH sont accessibles de l'extérieur. Cela nécessite d'autres outils pour assurer la sécurité et éviter l'intrusion. Tout d'abord les serveurs qui seront accessibles de l'extérieur devront être placés dans la DMZ, une zone démilitarisée, c'est-à-dire un réseau distinct des autres VLAN, ce qui a pour but en cas d'attaque de confiner celle-ci à cette zone et d'empêcher sa propagation au reste du réseau. A cela il peut être intéressant de coupler un *reverse-proxy*, permettant au serveur web d'être protégé des attaques directes de l'extérieur, ce qui renforce la sécurité du réseau interne. Enfin, le serveur de messagerie devra avoir une sécurité particulière, notamment pour se prémunir des « spams ». Il faudra donc mettre en place les antispams qui existent. Une autre réalité, est la nécessité d'accès distant des prestataires informatiques pour les mises à jour et maintenance de leur logiciel. Cela demande souvent l'utilisation d'un réseau privé virtuel (tunnel VPN) ou de louer une ligne spécialisée, le coût de cette solution étant très supérieur à la première.

3.6. *Sauvegarde des données et disponibilité du système*

Différents choix sont possibles pour la sauvegarde des données : archivage quotidien des données, sauvegarde des applications hebdomadaires, stockage sur bandes magnétiques ou sur disques externes, etc. A titre d'illustration nous mentionnons ici les choix techniques et le mode de fonctionnement adoptés par les centres hospitaliers partenaires.

Les serveurs ayant une partie « système et programmes » et une partie « données » à gérer, il faut envisager deux méthodes. La partie « système et programmes » est configurée à la mise en place du serveur ; son évolution est faible puisqu'elle est liée uniquement aux mises à jour. Pour ces éléments, il est souhaitable d'avoir une partition ou un disque dur dédié, et de réaliser une copie de sauvegarde une seule fois quand le paramétrage est validé et que le serveur est mis en « production ».

Les sauvegardes doivent permettre de garantir une restitution des données enregistrées après un crash technique ou une erreur de manipulation. Habituellement les sauvegardes se font de manière quotidienne et sont écrasées au bout de sept jours. Par conséquent on est capable de restituer des informations datant de 1 à 7 jours. Les sauvegardes sont faites manuellement avec des cassettes ou automatiquement, toujours avec un système de cassettes, mais géré par un robot de sauvegardes. Il est aussi possible de faire des sauvegardes à distances *via* un VPN par exemple. La disponibilité est la capacité du système à fonctionner malgré un incident technique. Par exemple un crash de disque dur ne doit pas empêcher l'utilisation d'un logiciel. Pour atteindre ces objectifs il faut combiner plusieurs méthodes :

– prévenir les problèmes liés aux défaillances de disque dur, il faut utiliser la technologie Raid. Cette technologie est basée sur la duplication des données sur plusieurs disques durs. Un disque dur « sain » peut ainsi prendre le relais au cas où le disque dur de travail devient « indisponible » ;

– concernant les systèmes et les applications, il faut être capable de travailler même si un serveur est globalement hors service. Pour cela, on peut utiliser des « fermes de serveurs », qui auront exactement les mêmes configurations initiales. En mode normal, ces serveurs se répartiront les utilisateurs *(Load Balancing),* alors qu'en fonctionnement dégradé, ils garantiront une continuité de fonctionnement ;

– concernant le local des serveurs, il y a des préconisations à suivre, telles que des normes incendies mais aussi la capacité de garantir un certain niveau de température, (autour de 23°C). Une température de 40°C peut avoir des conséquences rapides et violentes sur des serveurs. Remarquons aussi la nécessité que les serveurs soient connectés au réseau ondulé ou aient des onduleurs propres, pour ne pas souffrir de microcoupures inévitables entre une coupure de courant et une reprise par le groupe électrogène.

4. Conclusion

Le contexte de regroupement des plateaux médico-techniques implique une réflexion sur le remaniement ou l'adaptation du système d'information de l'établissement de santé. Le choix d'un nouveau système d'information demande de faire des choix technologiques, qui ne sont pas évidents lorsqu'on n'a pas la

connaissance des possibilités et des contraintes associées ; notamment pour une rénovation en profondeur du réseau informatique, l'accompagnement par une société de prestation de service est souhaitable. Les préconisations techniques proposées vont servir d'éléments de références dans la définition du besoin d'un établissement de santé dans un projet de modernisation de son système d'information et de celui associé au plateau médico-technique en particulier. Les enjeux et les risques associés à la mise en place d'un système d'information, ainsi que les facteurs clefs de réussite de projets de ces systèmes dans un établissement hospitalier ont été étudiés. Nous avons insisté sur l'aspect d'architecture web qui permet de répondre à des besoins primordiaux, et sur l'aspect sécurité qui devient un élément incontournable dans les systèmes d'informations souvent exposés à divers risques.

5. Bibliographie

Beuscart R., Grave C., Bricoteau D., Purro N., « Les étapes de définition d'un système d'information hospitalier : la place des utilisateurs », *Informatique et Santé,* Paris, Springer-Verlag France, vol. 13, n° 6, 1994, p. 765-795.

Bounekkar A., Deslandres V., Lemagny D., et Trilling L., « Etude des facteurs influençant le taux d'occupation des salles dans le contexte de regroupement de plateaux médico-techniques », *GISEH 2006*, 14-16 sept 2006, Luxembourg.

Castets P., « L'avenir de l'Hôpital et les systèmes d'information », *ARH info*, janvier 2004.

Charlet J., L'ingénierie des connaissances, développements, résultats et perspectives pour la gestion des connaissances médicales, Mémoire d'Habilitation à Diriger des Recherches, Université Pierre et Marie Curie, 2003.

Degoulet P., Fagon J.-Y., « Stratégies de mise en œuvre des systèmes d'information cliniques », *Gestion hospitalière*, 2004, p. 793-800.

Dinis A., Labrousse M., « Plateau technique et Système d'information », *revue Technologie de la santé,* n° 26, juillet 1996.

Fieschi M., « Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins », rapport ministériel, décembre 2003.

Grimes S.L., "The Future of Clinical Engineering: The Challenge of Change", *IEEE engineering in medicine and biology magazine*, March/April 2003, p. 91-99.

Henderson J.C., Venkatrman N., "Strategic alignment: Leveraging information technology for transforming organizations", *IBM Systems Journal*, 32, 1, 1993, p.4-16.

Jepsen T., "IT in Healthcare: Progress Report", *IT Pro magazine, IEEE Computer Society*, 2003.

Reichertz P.L., "Hospital information systems-Past, present, future", *International Journal of Medical Informatics*, 75, 2006, p. 282-299.

Verdier C., Cluze G., “Health care process based on the ABC model through a metastructured information system”, *ICEIS 2004.*

SAS – 10/2007. Systèmes d’information et santé, pages 65 à 81