ENSP
ECOLE NATIONALE DE LA SANTE PUBLIQUE

RENNES

Directeur d'Hôpital

Promotion 2004

L'émergence d'une politique de sécurité informatique au Centre Hospitalier Montperrin : jeux technico-organisationnels au croisement d'enjeux symboliques et matériels

Florence ARNOUX-LIOGIER

Remerciements

Nombreuses ont été les personnes qui m'ont aidée, conseillée, soutenue dans la rédaction de ce travail.

Je remercie tout particulièrement :

Mon maître de stage, Marie-Antoinette LAMPIS, pour son soutien indéfectible, ses conseils avisés, et sa maîtrise du principe de réalité,

Mon encadrant mémoire, Philippe PEYRET, pour ses critiques constructives et sa disponibilité confirmée jusqu'au dénouement,

Le directeur du Centre Hospitalier Montperrin, Jacques FRANCOIS, et son équipe de direction pour leur soutien chaleureux,

Toutes celles et ceux qui ont éclairé mon sujet de leur point de vue : Marguerite BAGAYOGO, Patrick BALDOUREAUX, Jeanne BOSSI, Etienne DUSEHU, Philippe FORNARI, Maximilien INTARTAGLIA, Marie-Thérèse LORIANT, Paul MILHON, Gérard MOSNIER, Jean-François POLLET (…) et tous ceux qui ont répondu aux questionnaires,

Toutes celles et ceux qui m'ont accompagnée dans la rédaction de ce travail, en particulier mes amis pour leur soutien moral et logistique et enfin mon sociologue de mari pour son intérêt intarissable pour le monde hospitalier.

Sommaire

Liste des sigles utilisés

ADESM	Association des Etablissements gérant des Secteurs de Santé Mentale
ANAES	Agence Nationale d'Accréditation et d'Evaluation en Santé
APHM	Assistance Publique Hôpitaux de Marseille
CH	Centre Hospitalier
CIM	Collège de l'Information Médicale
CHS	Centre Hospitalier Spécialisé
CHU	Centre Hospitalo-Universitaire
CME	Commission Médicale d'Etablissement
CNIL	Commission Nationale de l'informatique et des Libertés
CNOM	Conseil National de l'Ordre de Médecins
COPIL	Comité de Pilotage
CSP	Code de la Santé Publique
DIM	Département de l'information Médicale
DSIO	Directeur du Système d'Information et de l'Organisation
ENSP	Ecole Nationale de la Santé Publique
GMSIH	Groupement de Modernisation du Système d'Information Hospitalier
HUS	Hôpitaux Universitaires de Strasbourg
MCO	Médecine Chirurgie Obstétrique
PMSI	Programme de Médicalisation du Système d'Information
RSS	Réseau santé Social
RSSI	Responsable de la Sécurité des Systèmes d'Information
SDSI	Schéma Directeur du Système d'Information
SI	Système d'information
SIH	Système d'Information Hospitalier

INTRODUCTION

Affiché par le projet Hôpital 2007 comme l'un des trois thèmes essentiels (à côté des bâtiments et de l'équipement biomédical) à privilégier pour faciliter l'évolution de l'organisation de l'hôpital et de son environnement, le système d'information est un instrument essentiel de management opérationnel et stratégique des hôpitaux, dans le sens où il organise la saisie et la remontée des données indispensables à une prise de décision éclairée et efficace.

Conscient de l'évolution actuelle, pour ne pas dire de la mutation, des Systèmes d'Informations Hospitaliers (SIH), l'Etat a décidé, dans le cadre du plan Hôpital 2007, de l'octroi de 300 millions d'euros pour les études, le développement de logiciels et l'équipement.[1] A l'heure où le gouvernement entend accélérer la mise à niveau du parc informatique hospitalier, il convient de veiller à la protection des SIH. Car, comme le souligne le professeur Fieschi dans son rapport remis au Ministre de la santé en janvier 2003, « les systèmes d'informations hospitaliers sont faiblement sécurisés, cloisonnés, basés sur des applications verticales peu communicantes »[2]. Si certains hôpitaux ont intégré, depuis plusieurs années, une culture de sécurité fondée sur le caractère vital du système d'information, d'autres, comme le Centre Hospitalier (CH) Montperrin, s'inscrivent dans cette démarche depuis peu. Pour autant, ce dernier ne fait pas figure d'exception puisque, selon l'étude du CLUSIF[3] sur *Les politiques de sécurité des systèmes d'information et la sinistralité en 2003*[4], des politiques de sécurité ne sont définies que dans 42% des Centres Hospitaliers. Une des raisons nous est fournie par G MOSNIER, Directeur du CH Monfavet[5] et secrétaire général de l'ADESM[6] : « le système d'information a longtemps été mal appréhendé par les chefs d'établissement, et son importance commence à peine à être clairement perçue aujourd'hui ».

1 Système d'information, système informatique et sécurité

Apparue pour la première fois dans la circulaire du 16 novembre 1982, il faut attendre une circulaire de 1989[7] pour qu'une définition relativement précise de la notion de « Système d'Information Hospitalier » soit donnée par la Direction des Hôpitaux : « le

[1] D'ores et déjà, précisons qu'il ne s'agit là que de 3% des fonds « Hôpital 2007 » qui seront consacrés au SI ; le reste étant attribué aux équipements et surtout « au béton », ce qui démontre l'insuffisante prise en compte par les pouvoirs publics de l'impact organisationnel des technologies de l'information sur l'Hôpital, contrairement aux grandes entreprises qui, comme Eurocopter où nous avons fait un stage de deux mois, n'auraient pas hésité à investir massivement dans leur SI.
[2] Pr M. FIESCHI, Y. MERLIERE, *Les données du patient partagées : propositions pour l'expérimentation*, Note d'orientation au ministre de la santé, de la famille et des personnes handicapées, mai 2003.
[3] Club de la Sécurité des Systèmes d'Information Français.
[4] Consultable en ligne sur le site www.clusif.asso.fr. Les facteurs de sinistralité sont essentiellement les virus, les pannes internes, les vols, les erreurs d'utilisation, les évènements naturels.
[5] Spécialisé en psychiatrie, situé dans le Vaucluse. Entretien en date du 29 septembre 2004.
[6] Association des Etablissements gérant des Secteurs de Santé Mentale.
[7] Circulaire n° 275 du 6 janvier 1989 relative à l'informatisation des hôpitaux publics, *cf.* annexe II.

système d'information de l'hôpital peut être défini comme l'ensemble des informations, de leurs règles de circulation et de traitement nécessaires à son fonctionnement quotidien, à ses modes de gestion et d'évaluation ainsi qu'à son processus de décision stratégique ». Le SIH devient alors un outil incontournable pour la gestion administrative et médicale dans les établissements de santé. Le texte précise que l'objet de ce système d'information est de créer un tronc commun de données médicales et économiques pour analyser l'activité et élaborer des indicateurs utiles à la gestion. D'après H. DUFEY, Directeur du Groupement pour la Modernisation du Système d'Information Hospitalier (GMSIH), « les systèmes d'information serviront en quelque sorte de tableaux de bord, permettant l'accès rapide, voire en temps réel, aux résultats d'une activité, leur analyse, leur vérification et une correction de la trajectoire suivie si elle ne répond pas aux objectifs fixés. Le partage des données de santé devrait apporter des économies autour de 20 à 30 % des coûts totaux[8] ».

Un bon SIH est le résultat d'un bon système informatique hospitalier mais ne se réduit évidemment pas à la seule ressource informatique. Cependant, la partie non informatisée du système reste mal identifiée, y compris par les chefs d'établissements ou les Responsables des Systèmes d'Information et de l'Organisation[9] (RSIO, aujourd'hui plutôt dénommés Directeurs –DSIO- que responsables) qui confondent encore –ce qui est très révélateur - système d'information et système informatique[10].

Nous nous intéresserons, dans le présent mémoire, essentiellement au *système d'information informatisé* lequel organise de manière informatique la circulation de l'information dans l'hôpital et dépend de techniques matérielles et logicielles pour collecter, stocker, traiter l'information et la diffuser. Par ailleurs, notre étude s'inscrivant dans un champ pluridisciplinaire, nous envisagerons le système d'information hospitalier en tant que système socio-technique, dont la mise en œuvre implique de profonds investissements, voire bouleversements, sociaux, organisationnels et intellectuels. Notre réflexion tente en effet de tenir compte des spécificités de la structure concernée sous divers angles : technique, médical, psycho-social, environnemental, socio-économique. Il a été réalisé à partir d'une observation du terrain de référence : le Centre Hospitalier Montperrin, situé à Aix-en-Provence dans les Bouches du Rhône, établissement spécialisé en psychiatrie adulte et infanto-juvénile, en alcoologie et dans l'assistance aux toxicomanes. Disposant de plus de 550 lits et places, il regroupe environ 1500 agents en en intra et en extra-hospitalier[11].

---

[8] *Cf*. le rapport Fieschi, *Les données du patient partagées, op.cit.*
[9] *Cf*. Circulaire n°275, *op. cit.*
[10] *Cf*. PONCON G., *Le management du système d'information hospitalier. La fin de la dictature technologique*, Rennes, Editions de ENSP, 2000, chapitre 4 «Système d'information et systèmes informatiques », p. 48. L'auteur de l'ouvrage précise qu'il a réalisé une enquête entre septembre 97 et janvier 98 auprès de 76 chefs d'établissements ou DSIO, révélant que la moitié d'entre eux ne faisait pas la distinction entre système d'information et système informatique.
[11] Il comprend en effet une cinquantaine de structures extérieures répartie sur 34 sites distincts.

2 Sécurité informatique

Comme nombre d'organisations de santé confrontées à l'ouverture de leur système d'information, le CH Montperrin ne peut plus faire désormais l'économie d'une démarche active de modernisation dans ce domaine, compte-tenu notamment des évolutions majeures que connaît la psychiatrie depuis quelques années quant au genre de données collectées, à leur utilisation et à leur accès. En 2003, l'établissement a initié une démarche de sécurisation de son système d'information informatisé, essentiellement administratif et médico-technique, dans le cadre de l'ambitieux projet d'extension de ce dernier à l'ensemble de l'établissement. Cette réflexion sur la sécurité, en germe dans le schéma directeur du système d'information[12] actuel, doit s'intégrer dans la conception du prochain schéma 2005-2009.

La Direction du CH a fait appel à un cabinet d'audit pour l'accompagner dans cette démarche. Ce dernier a pour mission d'élaborer une politique de sécurité formalisée, une charte utilisateur et le schéma directeur (SDSI). Pour optimiser l'investissement dans ce projet, le modèle de gouvernance choisi a suscité la création d'une structure à l'échelle de l'organisation, un comité de pilotage (COPIL) représentant toutes les composantes de la communauté hospitalière[13] afin que la stratégie de l'hôpital soit adoptée par tous les groupes professionnels impactés. Un dialogue devait théoriquement être engagé à chaque niveau de la planification stratégique, mais la spécificité psychiatrique est, comme nous le verrons, venue contredire cet objectif.

3 Problématique générale

Le SIH du CH Montperrin reste encore trop inadapté aux besoins de l'établissement dans son ensemble et des professionnels dans leurs spécificités. Il ne va aujourd'hui guère au-delà de la simple gestion des données d'activité. Le CH est dépourvu d'unités de soins informatisées et ne s'est pas porté volontaire pour expérimenter le PMSI[14] psychiatrique.

Le projet de sécurisation du système d'information s'avère difficile et long à mettre en œuvre, dans la mesure où le CH dispose de deux environnements informatiques, ou

---

[12] La circulaire du 6 janvier 1989 (*op. cit.*) invite à définir un Schéma Directeur du Système Informatique (SDSI) afin d'évaluer les besoins en informatisation, les aspects organisationnels, techniques, économiques et financiers, et d'assurer le respect de la législation en vigueur, notamment la loi du 6 Janvier 1978 « informatique et liberté ». Ce SDSI est un plan d'actions transversal et pluriannuel, faisant partie intégrante du projet d'établissement actuel (1999-2004) et futur (2005-2009) et outil de pilotage nécessaire à la satisfaction des objectifs suivants : finalisation du déploiement de la filière administrative, pérennisation des actions déjà engagées (politique de sécurité, charte utilisateurs, etc.), mise en adéquation des infrastructures informatiques et de l'organisation de supports (rationalisation des moyens informatiques, cohérence des choix techniques, limitation des divergences entre informatique administrative et informatique médicale, organisation de la fonction informatique entre exploitation et gestion de projets).

[13] Administration, corps médical et soignant, personnels techniques et médico-techniques.

[14] Programme de Médicalisation des Systèmes d'Information, instauré en 1989 par la circulaire du 24 juillet pour les hôpitaux publics, et généralisé en 1995 dans l'ensemble du secteur hospitalier public et en 1997 dans le secteur privé, comme outil de financement des hôpitaux délivrant des soins aigus en Médecine Chirurgie Obstétrique (MCO). En sont exclues les consultations externes, l'hospitalisation à domicile, le long séjour, les maisons de retraite. Le PMSI est en cours d'expérimentation en psychiatrie et aux urgences (à l'exception des lits porte).

systèmes d'information, non interconnectés : le S.I. Administratif (SIA) sous la responsabilité d'un directeur d'hôpital et le S.I. Médical (SIM) sous la responsabilité du médecin-DIM[15], lequel exprime, aux côtés de quelques autres médecins, les plus vives réticences devant le projet de développement, d'unification et de sécurisation du SI, arguant du caractère irréductiblement confidentiel des données hébergées et traitées au sein du SIM. La constitution, dans les DIM des établissements psychiatriques, de fichiers nominatifs contenant des données sensibles représente d'après les médecins interrogés un danger collectif, danger souligné par un psychiatre et un psychologue dans un article du *Concours médical* : « la collecte et la transmission (…) de données personnelles, intimes et détaillées constituent une effraction dans le cadre des soins individuels et entravent gravement la relation de confiance, qui repose pour une grande part sur la confidentialité mise à mal »[16]. Le terme « effraction » mérite d'être souligné en tant qu'il illustre la résistance des médecins à communiquer, la volonté de cadenasser les informations médicales qu'ils détiennent. A Montperrin, les médecins n'adhèrent à cette logique de partage d'information qu'au niveau intra-sectoriel, et encore… Existe-t-il un particularisme de la psychiatrie qui justifie cette attitude ?

Les objectifs organisationnels relatifs au système d'information et à la politique de sécurité qui le sous-tend sont donc aujourd'hui déterminés par deux grands groupes d'acteurs qui se partagent un leadership dans ce domaine : la direction au sens large[17] et le corps médical.

Longtemps réduite à la notion de confidentialité, la problématique sécuritaire du Système d'Information est désormais reconnue par la majorité des acteurs du CH Montperrin comme majeure. Les médecins de l'établissement, y compris les réticents chroniques, commencent à être demandeurs d'outil informatique. Néanmoins, une résistance active de la part d'un petit nombre d'entre eux, chefs de service leaders et très respectés institutionnellement, a longtemps hypothéqué la mise en œuvre du projet. Notre hypothèse est que l'absence de consensus, qui a présidé au sein du CH Montperrin jusqu'à une période récente, tient officiellement au risque de remise en cause du secret médical, question particulièrement sensible en psychiatrie. Les médecins se sont arc-boutés sur ce dossier « politique de sécurité », qui n'est qu'un outil au service du SIH, d'une part parce qu'aucun consensus n'a émergé sur la question des données médicales partageables et d'autre part en raison d'une résistance culturelle devant l'échange

[15] Médecin responsable du Département de l'Information Médicale (DIM). La circulaire du 24 juillet 1989 marque le début de l'organisation de l'information médicale et de la généralisation du PMSI dans les hôpitaux publics. Elle met en place les premiers DIM dans les hôpitaux. Le DIM, composé de médecin(s) et de technicien(s) de l'information médicale, des secrétaires médicales le plus souvent, a un rôle d'aide au codage, de contrôle de la production, de formation, de groupage et d'analyse des informations médicales. Il s'occupe également de la gestion des dossiers médicaux et a par ailleurs un rôle de conseil et d'expertise, participant à ce titre à la conception du SI médical et du SDSI.

[16] GEKIERE C., MORVAN O, Du dossier patient aux « données du patient partagées », *Le concours médical,* 30 juin 2004, p. 1409.

[17] Direction proprement dite et Direction du Système d'Information et de l'Organisation –DSIO- essentiellement.

d'information, résistance que nous attribuons à la peur de voir l'information leur échapper. Or, le récent audit réalisé par le cabinet de conseil a mis en exergue les faiblesses du SIM (isolement, limitation des possibilités d'évolution en particulier), et son incapacité à garantir à lui seul la confidentialité des informations qu'il héberge. Nous verrons qu'un seul quiproquo et que l'absence de débat peuvent mettre en péril tout un projet, projet dont les aspects strictement techniques sont ici bien moins importants que les enjeux symboliques et matériels qu'il soulève.

4 Méthodologie et organisation de la réflexion

Nous nous intéresserons à la réalité technico-organisationnelle du système d'information. Nous utiliserons, pour ce faire, la sociologie des organisations et tenterons de rendre compte systémiquement[18] des circuits, réseaux, blocages éventuels, concentration, diffusion de l'information au sein du CH Montperrin. Notre investigation ne pourra dès lors pas se limiter à de simples considérations de faisabilité, d'efficacité technique et de pertinence juridique. Il nous faudra en effet tenter d'analyser les représentations véhiculées par les groupes d'individus concernés par la mise en place de ce système. Nous nous limiterons en l'occurrence, afin de circonscrire notre étude, aux personnels impliqués[19], bien qu'il serait tout à fait pertinent de tenir compte des représentations des usagers. En outre, nous inclurons dans cette approche technico-organisationnelle les aspects tenant aux objectifs de transparence, de démocratisation, d'éthique, qui apparaissent aujourd'hui comme des critères de « bonne gouvernance », autant que ceux tenant à l'efficacité humaine et à la rentabilité matérielle. Nous pourrons ainsi mobiliser, dans cette dernière perspective, les éléments collectés dans notre approche juridique, particulièrement ceux qui concernent les droits du patient en particulier. Les données recueillies à partir du croisement de ces trois méthodes (juridique, technico-organisationnelle et sociologique) permettront, du moins nous l'espérons, de mettre en exergue les difficultés rencontrées lors de la mise en place d'un système d'information sécurisé et à terme intégré voire, peut-être, de les dépasser en partie.

La recherche bibliographique nous a permis d'identifier et de recueillir les différentes données de référence, en particulier juridiques, en passant en revue les textes normatifs se rapportant de près ou de loin à la sécurité du système d'information et nous a ainsi amenée à distinguer plus clairement les rapports entre les champs technique et juridique dans le contexte hospitalier.

Nous avons ensuite mené une observation de terrain comprenant une enquête statistique par questionnaire fermé, afin d'évaluer le niveau de connaissance des

[18] C'est-à-dire en montrant les interdépendances entre phénomène social et logique d'organisation.
[19] Utilisateurs actuels du SIA et utilisateurs actuels et futurs du SIM.

utilisateurs concernant les bonnes pratiques de sécurité et leur ressenti dans ce domaine. Cette enquête consistait à identifier les représentations que les utilisateurs actuels ou futurs du système d'information se font de cet outil (imaginaire du réseau tentaculaire, de la fuite d'information, de la sophistication électronique incontrôlable ou contrôlée par les seuls «spécialistes », imaginaire à l'inverse de la machine intelligente qui remplace l'homme plus efficacement et règle tous les problèmes, cf. annexe I). Ces représentations constituent une des variables déterminantes du succès ou de l'échec de son déploiement. D'ores et déjà, nous pouvons préciser que le SIH est perçu essentiellement par l'ensemble des utilisateurs (SIA et SIM) comme un outil d' amélioration de la coordination et de la circulation de l'information de la prise en charge du patient et en même temps comme un réseau tentaculaire contrôlé par les seuls spécialistes. L'échantillonnage a été réalisé à partir de deux grands groupes d'acteurs[20] : celui des services administratifs (secrétaires, adjoints des cadres, attachés d'administration, directeurs, etc.), celui des personnels de trois unités de soins pilotes pour l'informatisation (secrétaires médicales, aides-soignantes, personnel médico-technique, infirmiers, cadres soignants, médecins, assistantes sociales, psychologues) et de trois unités non pilotes. L'enquête transversale a été menée simultanément au sein des deux groupes, le questionnaire ayant étant anonymé lors de l'exploitation. Nous avons prolongé notre étude de terrain par des entretiens non directifs effectués sur sites[21] et par téléphone, à partir de différents questionnaires ouverts dont nous avions adapté le contenu au statut et aux fonctions de l'interlocuteur. Précisons d'ores et déjà que la majorité des entretiens réalisés au sein du CH Montperrin ont été anonymés, soit à la demande de nos interlocuteurs soit en raison de la nature « sensible » des propos tenus. En outre, nous nous sommes intéressée aux expériences d'autres établissements : trois établissements psychiatriques de la région[22] ainsi que des centres hospitaliers généraux[23] et universitaires[24] qui sont en cours d'élaboration d'une politique de sécurité ou qui ont été précurseurs en la matière. Bien que non systématiquement comparables en terme de taille ou de spécialisation, il nous a semblé intéressant d'analyser l'attitude des utilisateurs de ces SIH, les obstacles éventuels à la sécurisation, et les solutions éprouvées.

Pour évaluer les conséquences de telles mutations organisationnelles au sein d'un hôpital, il nous semblait en effet indispensable de s'intéresser à la représentation des agents qui échangent au quotidien des techniques, des savoirs et des savoir-faire. A partir de cette démarche globale, nous avons tenté de dégager une problématique, de cerner les freins et les éléments facilitateurs d'ordre technique, juridique ou de nature plus

[20] Au sens de CROZIER M., et FRIEDBERG E., *L'acteur et le système*, Ed. du Seuil, 1977.
[21] Au sein du CH Montperrin et dans d'autres établissements MCO et spécialisés en psychiatrie.
[22] CH Valvert et CH E. Toulouse dans les bouches du Rhône ; CH Montfavet dans le Vaucluse.
[23] CH Intercommunal de Fréjus Saint Raphaël en particulier.
[24] Hôpitaux Universitaires de Strasbourg (HUS), CHU de Montpellier et Assistance-Publique-Hôpitaux-de-Marseille (APHM).

informelle rencontrés au cours de la concrétisation du projet, les stratégies poursuivies par les acteurs, ceci afin de mettre au jour des solutions de sécurité techniques, organisationnelles, fonctionnelles de nature à gagner ou restaurer la confiance des utilisateurs. Nous espérons ainsi délivrer quelques propositions tirées de l'analyse des avantages et effets à court et moyen terme rencontrés par ces hôpitaux en matière d'amélioration de la sécurité, aux différents stades de l'implantation et du développement de leur système d'information.

Notre étude nécessite d'identifier les dimensions de l'organisation et de la gestion du SI, système d'information que nous présenterons de façon générale, sans entrer dans les détails techniques que seules des connaissances en informatique permettent d'appréhender précisément. Après avoir mis en évidence dans une première partie les caractéristiques du système d'information actuel, l'architecture cible, le socle normatif qui sous-tend la politique de sécurité conçue comme un instrument au service du SIH, nous essaierons de comprendre dans une deuxième partie en quoi la refonte du SI au CH Montperrin et le projet de politique de sécurité bouleversent l'ordre établi et font surgir de nouvelles questions socioculturelles, éthiques, médico-économiques. Nous tenterons dès lors de cerner les freins propres à l'organisation hospitalière et à la psychiatrie après avoir présenté depuis sa genèse jusqu'à son dénouement ce projet de sécurisation informatique. Il nous semble que ces blocages se retrouvent à des degrés divers dans beaucoup d'établissements de santé, se caractérisant par exemple par un manque de confiance dans les technologies nouvelles, en particulier dans l'informatique et la mise en réseaux des données médicales ou encore et surtout par la difficulté à partager les informations, nombre de médecins craignant une interaction entre les données administratives et les données purement médicales. On ne peut certainement pas appréhender ce qui se joue ici sans saisir ce que signifie théoriquement et pratiquement à l'hôpital la distinction entre les dimensions administratives et médicales, sans saisir ce que recouvrent de malentendus les notions de secret médical, de confidentialité, de transparence, de besoin de partage, de système transversal etc. La troisième partie sera consacrée à la politique de sécurité proprement dite, c'est à dire au choix de solutions technico-organisationnelles (dans lesquelles nous englobons les aspects humains) permettant d'assurer la confidentialité, l'intégrité et la disponibilité du SIH. Il sera intéressant de s'interroger sur la façon dont la mise en place de cette politique va affecter les pratiques et relations professionnelles et sur les méthodes qui sont ou pourraient être employées afin d'emporter l'adhésion des agents concernés par le projet et la mobilisation optimale de leurs compétences et savoir-faire. Nous verrons alors comment une politique de sécurité informatique diffusée à l'échelle de l'hôpital peut devenir un outil puissant de changement organisationnel, sur le plan de culture et de la structure.

1 LA POLITIQUE DE SECURITE INFORMATIQUE, INSTRUMENT AU SERVICE DU SYSTEME D'INFORMATION CIBLE

L'étude du thème de la sécurité informatique doit nécessairement partir d'une analyse critique du système d'information existant, dans toutes ses dimensions technique, organisationnelle et humaine ainsi que d'une évaluation prospective de ses possibilités d'évolution.

1.1 Un projet de management conciliant préservation et optimisation des acquis

Le détour par l'analyse du système d'information existant[25] et, particulièrement, de sa dimension informatique, devrait permettre non seulement de cerner les avancées réalisées, leurs limites, les besoins encore insatisfaits et les enjeux de la mutation et de la sécurisation du SI, mais encore d'appréhender les modalités de conciliation de ce dernier avec le projet d'établissement et l'environnement extérieur, conciliation essentiellement assurée par le schéma directeur.

1.1.1 Le SIH : une vitrine de l'hôpital

Pour aborder la problématique de la sécurité du système d'information, il est essentiel, en particulier pour un cadre de direction, de saisir les liens étroits qui relient gestion, organisation et système d'information.

A) Caractère stratégique de la maîtrise du système d'information

a) L'interdépendance entre système d'information et organisation hospitalière

Les rapports entre société et technologie sont de plus en plus complexes, les technologies de l'information et de la communication jouant un rôle dans la gestion et la structuration des relations sociales quotidiennes et la nature même de l'ordre social. La technique investit le champ du changement social[26], l'utilisateur est de plus en plus dépendant de cette dernière[27].

Quatre étapes marquent le développement des systèmes d'information hospitaliers : l'informatisation des activités administratives (gestion administrative des

[25] Soit les moyens humains, matériels, les règles de circulation et de traitement, les modes de gestion et d'évaluation, les processus de décision stratégique, *cf.* Circulaire du 6 janvier 1989, *op. cit.*

[26] Nous n'employons pas ici le terme « champ » au sens ou l'entend P. BOURDIEU ; en effet, selon ce dernier, le champ est un espace social qui peut être appréhendé dans une perspective dynamique, mais aussi statique, ce qui exclurait toute conception du changement social comme espace social, c'est-à-dire comme champ.

[27] *Cf.* sur cette idée, l'intervention de GRANJON F., sur la « Socialisation de la technique, technicisation de la société : quelle(s) sociologie(s) ? Propositions pour une analyse critique des usages sociaux des technologies de l'information et de

malades, des ressources etc.), la construction d'un système d'information de gestion hospitalière[28], l'informatisation des activités médicales, et dans un dernier temps, l'intercommunication des données médico-administratives. Force est de reconnaître que le CH Montperrin, comme beaucoup d'établissements, n'a franchi que la première étape.

Selon H. DUFEY[29], le système d'information représente à peine 0,8% à 1,4% du budget d'exploitation hospitalier. Or, sa mise en œuvre, son déploiement et sa sécurisation réclament des moyens et des ressources importants. En tant qu'ensemble des moyens permettant aux informations de parvenir à ceux qui en ont l'utilité, «il est donc la somme d'une organisation fonctionnelle, de processus et d'un système informatique »[30].

Toute approche du SI doit être liée à la réflexion sur l'adaptation des organisations et des pratiques, notamment par la mise en place progressive des pôles d'activité, afin de décloisonner l'organisation, favoriser un pilotage décentralisé et rapprocher les logiques médicales des logiques de gestion. La réflexion menée au sein du CH Montperrin sur la logique des pôles n'étant pas encore passée au stade de la mise en œuvre pratique, cette notion institutionnelle ne sera pas prise en compte dans notre étude.

Les décisions en matière d'infrastructure sont d'autant plus efficaces qu'elles sont directement reliées aux stratégies de l'organisation hospitalière qui sont retracées notamment dans son projet d'établissement. En ce sens, un système d'information est un instrument au service d'une stratégie managériale et de transversalité, en tant qu'il fait partie de la mise en œuvre du projet d'établissement.

Le CH Montperrin ne bénéficie pas des mesures incitatives promises par la plan Hôpital 2007 au titre de l'investissement hospitalier, aucun des dossiers présentés dans la région PACA n'ayant été retenu. Il finance, sur son budget propre, les investissements relatifs aux matériels, réseaux, logiciels. Compte tenu des besoins dans ces domaines, il paraît difficile de respecter le planning prévisionnel annoncé.

b) Un système au service de l'organisation

Le SIH fait partie intégrante de la politique organisationnelle du seul fait qu'il gouverne l'accès à une ressource-clé du fonctionnement de l'établissement hospitalier : l'information. Il s'agit en effet d'un ensemble de composantes intrinsèquement liées qui recueillent, traitent, stockent et diffusent de l'information afin de soutenir la prise de décision, la coordination, la communication, le contrôle et l'analyse au sein de l'hôpitalIl a

---

la communication », Groupe de travail n°13, 17ème congrès international des sociologues de langue française, Tours, 5-9 juillet 2004.

[28] Rappelons que c'est avec le PMSI que s'introduit au début des années 80 la notion de gestion de l'information.

[29] Directeur du GMSIH.

[30] Extrait d'un article de JONCOUR M., Directeur du Syndicat Informatique Hospitalier de Picardie, Produire de la valeur, *DH magazine*, mai-juin 2004, n°95.

pour vocation d'optimiser les flux d'informations et de connaissances au sein de l'hôpital et d'aider les gestionnaires à tirer profit des ressources communiquées. Il est enraciné dans l'organisation hospitalière en ce qu'il interagit avec ses éléments clés : structures, procédures, politiques et culture. Par exemple, la culture de l'hôpital, tournée vers la satisfaction du client et la qualité de la prise en charge produit des effets sur la structuration du SI.

Qu'il s'agisse d'organiser des activités de production ou de service, d'en assurer le contrôle comptable et administratif ou de faciliter la prise de décision, les dispositifs de gestion et de management dépendent des informations[31] renseignant sur la répartition institutionnelle des tâches et fonctions, leur nature, leur durée et leur coût.. Le traitement informatisé de l'information s'inscrit dans un mouvement de rationalisation et de codification des informations circulant dans l'organisation. En tant qu'ensemble organisé des ressources matérielles et humaines, le système d'information assiste l'analyse, la gestion, la planification et la prise de décision. De ce fait, le système d'information apparaît comme étant un vecteur de rationalisation des activités collectives qu'il collecte et transcrit. Ce «système nerveux » contribue à la gestion des opérations quotidiennes, fournissant des indicateurs de fonctionnement et d'évaluation et offre la possibilité d'une véritable gestion stratégique. En gérant la complexité, il donne sa cohérence à la structure et favorise l'émergence de pratiques plus transversales et coopératives. L'informatisation du suivi des trajectoires des patients, la mise en place de guides de bonnes pratiques et de référentiels constitue un socle fiable et efficace pour la coordination, la continuité et la qualité des soins, en s'appuyant sur la traçabilité et le partage des informations. Les systèmes d'information ont donc un rôle déterminant à jouer pour améliorer la qualité de la prise en charge à l'hôpital et plus largement celle des systèmes de santé. Une politique de sécurité doit donc pour ce faire être compatible avec la culture, la structure et les objectifs de l'organisation. L'informatisation facilite la circulation des données et accentue la fiabilité et la sécurité de la transmission. Elle induit dès lors un accès restreint à l'information ainsi qu'une optimisation de la qualité de gestion : l'outil informatique n'est plus aujourd'hui un simple outil de bureautique. Le système d'information naît avec l'organisation et s'aligne stratégiquement sur ses objectifs, au nombre desquels l'amélioration de la qualité des soins et la maîtrise des coûts.

c) La nécessité de piloter le patient dans un système de soins complexe

L'amélioration de la prise en charge du patient est au centre de toute réflexion sur l'élaboration et la perfection du système d'information et appelle une évolution culturelle

[31] L'information peut revêtir un aspect administratif (bon de commande), médical (dossier patient) ou encore technique (mode d'emploi).

de l'appréhension de la question des dossiers patients partagés et de leur future informatisation. « Les SIH sont les points d'ancrage naturels des dossiers des patients et de la production de soins lourds. Leur mutation vers des systèmes centrés patient, modernes, flexibles et interopérables est une nécessité pour l'informatisation des processus de soins », soulignent M. FIESCHI et Y. MERLIERE.[32] Or c'est au cœur de la politique de sécurité que doit être placé le patient, par la recherche continuelle d'un compromis acceptable entre impératifs d'efficacité du soin et impératifs de sécurité de l'information satisfaits par le respect du droit à la vie privée[33] du patient et l'assurance de la confidentialité[34] des informations médicales.

L'objectif ultime du schéma directeur des systèmes d'information est d'assurer, à terme, la convergence entre l'informatique administrative et l'informatique médicale dans une direction plaçant le patient au cœur du système d'information et permettant sa gestion unique tout en assurant une utilisation efficace des ressources, tant humaines que financières, investies par l'établissement. Le SIH sécurisé doit répondre aux besoins en matière d'information de tous les corps de métiers et les aider ainsi dans leurs pratiques professionnelles. Ce système doit donc être centré plus que jamais sur le patient, cet « électron libre » qu'il faut pouvoir situer dans tous les aspects de sa prise en charge, dans les filières de soins et dans les réseaux au-delà de l'établissement. Il doit également être centré sur la gestion de la production des soins, intégrant les projets de réorganisation interne tels que les pôles d'activités. En effet, les pôles, en tant que centres de décision, auront un impact important sur le SIH. L'information est rarement concentrée en un seul endroit, en raison du nécessaire partage d'information entre les différents professionnels de santé. Le système d'information doit contribuer à améliorer la qualité des prestations dispensées auprès des patients, qu'elles soient de nature médicale, médico-technique, soignante, administrative. Un SI efficace devient dès lors une garantie de la qualité, de l'intégrité[35] et de la confidentialité des informations. Un défaut majeur relevé dans les établissements est le manque de communication des applicatifs[36], ce qui freine la bonne circulation des données dans le SI. Encore faut-il faire prendre conscience aux gestionnaires, soignants et médecins du caractère hautement stratégique de la maîtrise et de l'optimisation du SI. Selon H. DUFEY, directeur du

---

[32] *Les données du patient partagées* , *op. cit.* p. 41.

[33] *Cf*. article 2 de la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie : « Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant ».

[34] *Cf*. Charte du patient hospitalisé du 6 mai 1995, loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, la loi n° 78-17 (*op. cit.*), loi du 17 juillet 1978 modifiée d'accès aux documents administratifs, code civil (article 9), loi n°90-527 du 27 juin 1990 relative aux droits et à la protection des personnes hospitalisées en raison de troubles mentaux, Convention européenne des droits de l'homme, code pénal (articles 226-13 et 226-14 relatifs au secret professionnel), loi du 13 juillet 1983 modifiée, relative aux droits et obligations des fonctionnaires (article 26, discrétion professionnelle), loi 2004-801 (*op. cit.*).

[35] L'information est transmise sans être copiée ou modifiée.

[36] Logiciels de gestion financière et comptable, de gestion des ressources humaines, de gestion économique et logistique, de paye, de gestion du patient, d'analyse de gestion et de comptabilité analytique etc.

Groupement pour la Modernisation du Système d'Information, de plus en plus d'établissements s'intéressent à la sécurité des informations, comme l'illustre leur investissement croissant dans les projets du GMSIH[37].

Depuis la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé[38], qui garantit au patient la propriété de son dossier médical auquel il peut accéder directement[39], la nécessité se fait plus grande de réorganiser le SI autour du patient. Cette loi induit des conséquences sur la sécurité des SI de santé qui devraient être traitées dans les prochains décrets d'application.

B) Un centre nerveux à protéger sous quatre angles

La sécurité des informations doit être accrue car les supports de transmission informatisés accentuent les possibilités de rupture de confidentialité et de récupération des données, à des fins commerciales notamment.

Une révolution en cours se joue actuellement au travers de la dématérialisation des fichiers, des données, des titres (assurance maladie), des appels d'offres qui influent sur l'ouverture du système d'information, aujourd'hui encore insuffisamment développée. Cette ouverture sur l'extérieur postule un renforcement de la sécurité informatique et une réflexion approfondie sur les notions d'habilitation, d'autorisation, d'assurance, de secret professionnel et plus particulièrement sur les volets qui composent la sécurité : intégrité, confidentialité, disponibilité, auxquelles nous ajouterons la traçabilité/auditabilité. Le tableau suivant spécifie les besoins de sécurité en fonction des objectifs de sécurité correspondants.

[37] Créé par la loi du 27 juillet 1999 portant création de la CMU.
[38] N° 2002-2003 du 4 mars 2002, J.O du 5 mars 2002, dite « Loi Kouchner ».
[39] Décret d'application 2002-637 du 29 avril 2002.

Exigences majeures de sécurité = *Préoccupations PREMIERES*		Besoins de sécurité = *Axes de protection*			
		Disponibilité	Intégrité	Confidentialité	Auditabilité
Objectifs de sécurité = *Axes de sensibilité*	Respect de l'intimité des personnes et des libertés individuelles		***Préoccupation PREMIER E***	***Préoccupation PREMIERE***	
	Accessibilité aux postes de travail (dédiés ou partagés)			***Préoccupation PREMIERE***	***Préoccupation PREMIERE***
	Accessibilité aux réseaux informatiques (dans, depuis, vers CHM)	***Préoccupation PREMIERE***			***Préoccupation PREMIERE***
	Accessibilité aux informations et aux ressources informationnelles	***Préoccupation PREMIERE***	***Préoccupation PREMIERE***	***Préoccupation PREMIERE***	***Préoccupation PREMIERE***

a) La confidentialité des données, une notion d'une extrême importance en psychiatrie

La protection de la confidentialité postule que seuls les utilisateurs habilités, dans des conditions strictement déterminées, ont accès aux informations. Le respect de la confidentialité s'appuie sur un cadre législatif et réglementaire[40], des normes et recommandations qui émanent du secteur médical et du secteur de la sécurité des systèmes d'informations.

La confidentialité est indispensable à tout SIH, en particulier médicalisé ; c'est celle qui retiendra le plus notre attention en raison de son importance en contexte psychiatrique et de la rigueur de la législation en ce domaine. Elle est définie par le manuel d'accréditation de l'ANAES (2ème version)[41] comme « la propriété d'une information qui n'est ni disponible ni divulguée aux personnes, entités ou processus non autorisés ». Elle fait ainsi référence à la norme NF ISO 7498-2[42] concernant le système de traitement de l'information.

On peut recenser divers types d'atteinte à la confidentialité : vol, erreur, volontaires ou non, de manipulation dirigeant des informations vers le mauvais destinataire, accès indiscret, usurpation d'identité, copie de fichiers, interception de transmission. Pour protéger la confidentialité du système et des données, les protections physiques et logiques doivent être efficaces. Si la rupture de la confidentialité se constate à l'hôpital général tous les jours, la psychiatrie tente d'éviter cet écueil. Il est intéressant de noter

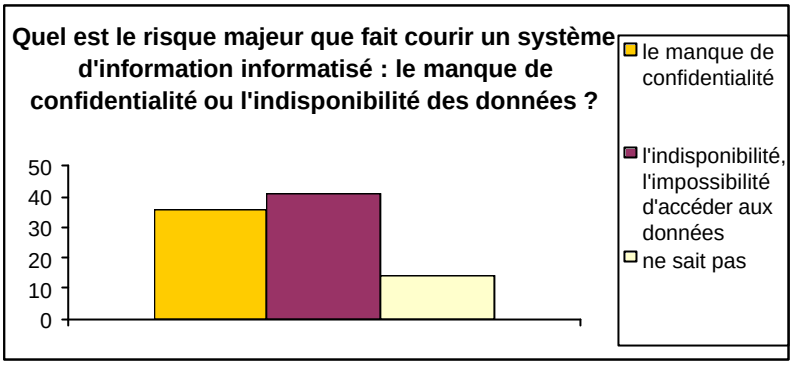
[40] Enoncés par la Charte du patient hospitalisé du 6 mai 1995, la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, la loi n° 78-17 du 6 janvier 1978 relative à l'information, aux fichiers et aux libertés, la loi du 17 juillet 1978 modifiée d'accès aux documents administratifs, le code civil (article 9), la loi n°90-527 du 27 juin 1990 relative aux droits et à la protection des personnes hospitalisées en raison de troubles mentaux, la Convention européenne des droits de l'homme, le code pénal (articles 226-13 et 226-14 relatifs au secret professionnel), la loi du 13 juillet 1983 modifiée, relative aux droits et obligations des fonctionnaires (article 26, discrétion professionnelle).

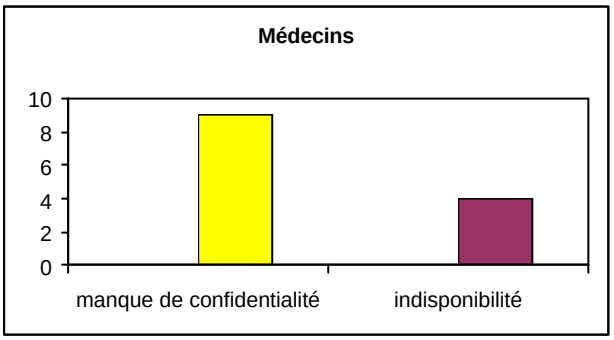
[41] Référentiels 4, 27, 37, 43d du manuel d'accréditation : la confidentialité et la sécurité des informations doivent être garanties tout au long du parcours du patient au sein de la structure.

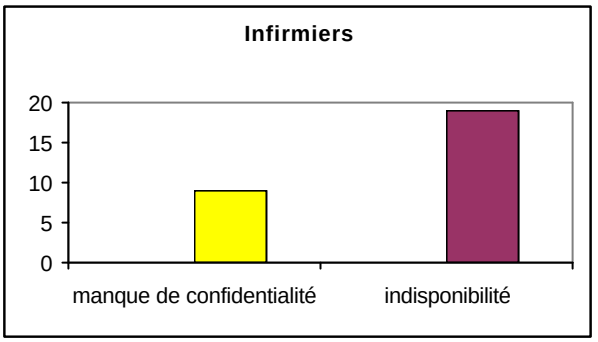
[42] De septembre 1990.

que les professionnels de santé, et en particulier les soignants, jugent pourtant la rupture de confidentialité moins grave que l'indisponibilité des données, à l'exception du corps médical qu s'inscrit diamétralement dans le sens contraire.

Utilisateurs du SIM :

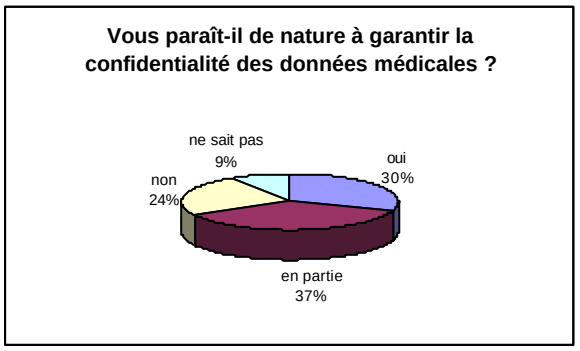




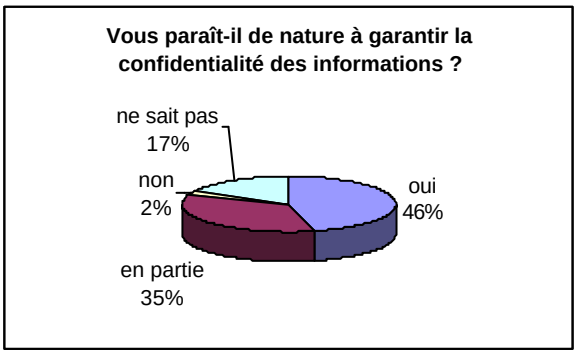


Par ailleurs, les utilisateurs du SIM ne sont que 30 % à considérer que le circuit actuel de l'information (papier, fax, téléphone) est de nature à garantir totalement la confidentialité des informations contre 46% des utilisateurs du SIA :

SIM



SIA

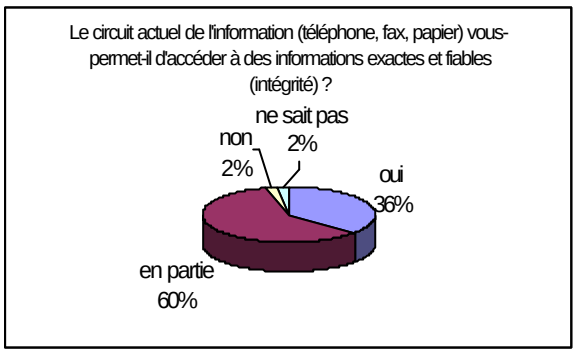


b) L'intégrité des données

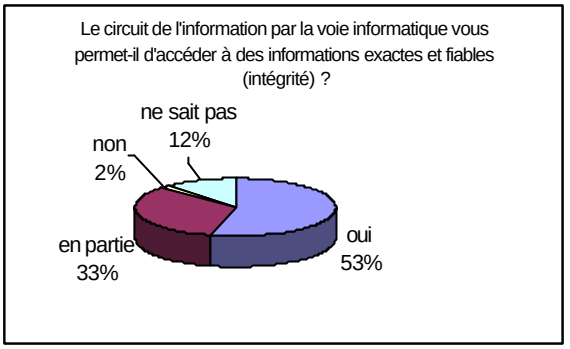
L'intégrité, c'est-à-dire le caractère complet, l'exactitude parfaite de chaque information, suppose qu'une information ne peut être modifiée que par les utilisateurs habilités, dans des conditions déterminées.

L'atteinte à l'intégrité peut prendre les formes énoncées plus haut au sujet de la rupture de confidentialité ainsi que le contrôle des écritures, des traitements et des transmissions des données.

SIM



SIA



L'enquête révèle que seulement 36 % des utilisateurs du SIM estiment accéder à des informations totalement exactes et fiables, contre 53 % des utilisateurs de l'informatique administrative.

c) La disponibilité du système

La sécurité des informations confiées par les patients conditionne la confiance accordée par le patient au médecin. Cette sécurité doit être conciliée avec la disponibilité des informations, indispensable à la qualité et à la continuité des soins.

La continuité est nécessaire à la disponibilité des données et services informatiques, dans les conditions d'accès et d'usage (notamment pour les performances) normalement prévues. L'indisponibilité résulte soit d'atteintes portées à l'intégrité des informations au niveau des données, des logiciels ou des matériels, soit d'une défaillance de l'environnement technique et humain nécessaire à son fonctionnement. Ceci implique concrètement l'organisation de tours de garde et d'astreinte pour les personnels.

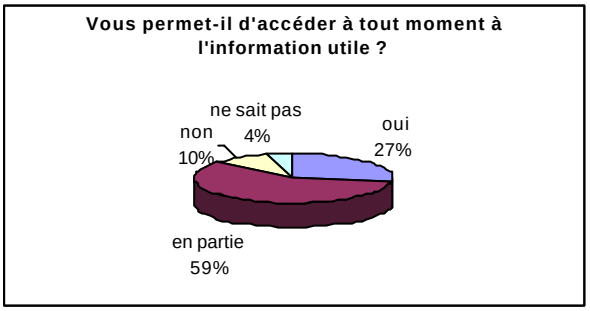
La future médicalisation du système d'information montperrinois conduira à réfléchir aux problèmes de continuité et à envisager notamment l'hypothèse de l'inaccessibilité d'un dossier médical informatisé à un instant où il serait urgent voir vital de le consulter. Bien que la perspective d'une informatique médicale et d'un dossier médical informatisé paraisse encore lointaine – la DSIO n'envisage pas la concrétisation d'un tel projet avant cinq ans, compte tenu de la maturité de l'établissement –, le CH doit commencer à étudier cette hypothèse pour y apporter une ou plusieurs réponses.

Au CH Montperrin, la réflexion porte actuellement essentiellement sur les moyens nécessaires à la continuité de la transmission des informations : recrutement d'un chef de projet, reconfiguration des fiches de poste, astreintes, maintenance des matériels. La sécurisation de l'architecture matérielle participe de la continuité du système, continuité

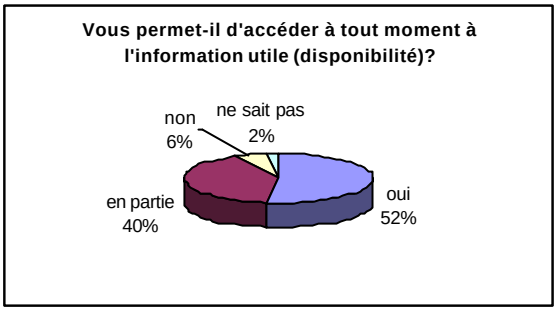
rendue indispensable une fois la médicalisation du système d'information mise en œuvre. Le choix a été fait d'installer un second serveur dans un local aménagé et climatisé, ainsi qu'un système de sauvegardes journalières. Si elles n'évitent pas les pannes, ces deux innovations assurent néanmoins la continuité de fonctionnement du service informatique**.**

Un système d'information médico-administratif informatisé entièrement sécurisé ainsi que le futur dossier médical partagé informatisé devraient contribuer à améliorer les liens entre l'intra et l'extra hospitalier – deux environnements actuellement non reliés si ce n'est par les outils de télécommunication classiques (téléphone, télécopie) – et, ainsi, mieux assurer la continuité du soin et de la prise en charge et le partage de données fiables.

SIM



SIA



Nous constatons qu'au CH Montperrrin, le circuit actuel de l'information (oralité, fax, papier) ne permet qu'à 27% des utilisateurs d'accéder à l'information utile, contre 52 % des utilisateurs de l'informatique administrative.

d) L'auditabilité et la traçabilité

Il s'agit de la capacité pour un SI de permettre des analyses complètes et simplifiées et de retrouver les informations et/ou les traces d'une erreur ou d'une intrusion.

L'authentification et la signature, notamment par la CPS, permettent de tracer de manière irréfutable l'utilisateur, qui est averti de cette traçabilité. Cette trace peut être auditée par les responsables et conservée.

Le SI est longtemps resté le « parent pauvre » à l'hôpital, car il ne pouvait rivaliser, en raison d'un manque de visibilité, avec l'investissement immobilier notamment. L'établissement accuse un retard en matière de système d'information (médical essentiellement) informatisé et en particulier en ce qui concerne sa sécurité. A Montperrin, cette « sinistrose de l'informatique », comme l'a nommé l'un des membres de la DSIO[43], serait en partie due, selon ce dernier, à une « gestion familiale et paternaliste » par la Direction. Nous identifions d'autres raisons de ce retard : faiblesse des maîtrises

d'ouvrage, formation insuffisante, mauvaise expression des besoins, investissements insuffisants et, concernant la sécurité en particulier, une mauvaise perception de la rentabilité, mais aussi et surtout un cloisonnement des deux SI en présence (SIA et SIM).

1.1.2 Un retard technique entretenu par une déconnexion des deux SI

Le système d'information du Centre Hospitalier Montperrin s'est construit progressivement en fonction des besoins de gestion exprimés par les acteurs du domaine hospitalier. Il est caractérisé par une informatique administrative et médico-technique en voie de maturité et ayant connu des évolutions récentes et une informatique médicale s'appuyant essentiellement sur des outils bureautiques. A ce jour, il n'existe pas de communication informatique, de réseau entre ces deux environnements.

A) Un système d'information orienté sur le traitement centralisé des données administratives et médico-techniques

a) Une informatique administrative techniquement opérationnelle en matière de sécurité

Le SIA regroupe l'ensemble des activités de l'hôpital à l'exception des activités médicales. Les données transmises, analysées et partagées de manière informatisées sont essentiellement comptables (actes et dépenses), socio-démographiques.

Actuellement, les ressources informatiques sont essentiellement concentrées dans les services administratifs, à l'exception des secrétariats médicaux. Le CH dispose d'un seul réseau informatique «physique »[44] qui repose sur des «sous-réseaux » (Internet, « commun », administratif, messagerie électronique, etc.) communiquant entre eux au travers d'un pare-feu. Jusqu'à ces derniers mois, ce réseau couvrait uniquement les bâtiments administratifs. Il est aujourd'hui en cours d'extension aux unités de soins en intra-hospitalier, les derniers pavillons devant être câblés avant la fin de l'année 2004. Mais ce type de réseau est vulnérable, car toutes les communications entre les points du réseau doivent passer par l'ordinateur central. Plusieurs réseaux logiques, étanches entre eux et indépendants, sont installés sur ce réseau physique. Un réseau logique « commun » permet la cohabitation de services partagés par les différents réseaux logiques (messagerie, Internet, intranet, logiciel de gestion des médicaments). A côté des applicatifs orientés métier (gestion financière, GRH, gestion administrative du patient), quelques applications périphériques existent : au laboratoire pour les résultats, à la pharmacie pour la dispensation nominative et pour les statistiques. La pharmacie et le laboratoire sont informatisés, sans toutefois être interconnectés avec les unités de soins.

---

[43] A l'occasion d'un entretien en date du 05 août 2004.
[44] de type étoilé mais non maillé, constitué d'un ordinateur central, relié à plusieurs ordinateurs ou terminaux.

Les demandes d'analyse, de médicaments ou encore de résultats sont transmises par papier ou par fax en l'absence de système informatique mis à la disposition des soignants qui utilisent principalement des applications bureautiques.

Globalement, le niveau opérationnel de sécurité des infrastructures supportant le système d'information du Centre Hospitalier Montperrin peut être considéré comme satisfaisant. En effet, certaines règles de base en matière de sécurité-réseau ont été définies, *a minima* formalisées et mises en œuvre. Néanmoins si les mesures techniques existent, elles n'étaient pas globalement, jusqu'à ces derniers mois, formalisées ni suivies (plan de secours, politique de sécurité, audits).

b) Un « domaine » administratif protégé

Le « domaine » administratif est rattaché à un serveur unique[45] contenant la base d'annuaire auquel chacun doit s'adresser pour l'authentification et l'accès aux ressources.

L'administrateur du domaine en assure la gestion et possède tous les droits. Lorsqu'un utilisateur allume son poste de travail, il s'identifie sur le domaine pour ouvrir une session de travail. L'authentification réussie lui ouvre alors des droits d'accès permanents aux ressources pendant la durée d'ouverture de la session. Les fichiers bureautiques partagés ne sont pas inscrits sur les disques durs locaux mais sont centralisés sur des serveurs de fichiers, lesquels font partie intégrante du domaine.

c) Analyse comparative

Il convient néanmoins de relativiser ce retard au regard de l'état des lieux réalisé par le GMSIH en 2001 qui montre que les établissements de santé sont assez mal armés pour démarrer ou étendre leur politique de sécurité. Une analyse comparative des SI d'autres établissements nous a permis de découvrir un fond sonore commun et de relativiser le retard du CH Montperrin.

Le Centre Hospitalier psychiatrique de Montfavet, situé dans le Vaucluse, a débuté une informatisation intensive en 1998 et concrétise actuellement son deuxième schéma directeur informatique (2003-2007). Un des axes de stabilisation adopté par ce schéma est la mise en œuvre d'une politique de sécurité par la définition et la définition de procédures et d'une charte de sécurité. Il a également institué un comité de veille informatique et un comité de sécurité informatique. Le système d'information couvre l'ensemble des activités de l'établissement (médico-administratives) et favorise une approche et une utilisation coordonnées et efficaces de l'information, notamment pour la

[45] Il s'agit du domaine *Active Directory*, composé d'un serveur principal et deux serveurs auxiliaires, comprenant un service d'annuaire centralisé contenant les informations concernant les objets réseaux (imprimantes, utilisateurs, applications, pc...) et doté d'une gestion centralisée pour l'authentification et l'accès à ces objets réseaux. Tous les objets sont protégés par des listes de contrôle d'accès (ACL), attribuées par l'administrateur du domaine, lesquelles déterminent qui peut voir un objet et quelles actions chaque utilisateur a le droit d'effectuer sur l'objet.

politique d'évaluation. Les services de soins du CH Valvert, situé à Marseille et spécialisé également en psychiatrie, en sont, quant à eux, à leur troisième schéma directeur du SI. Ces services sont informatisés, les outils techniques mis en place paraissant déjà très complets d'un point de vue fonctionnel et géographique. Le dossier médical étant informatisé, l'établissement est prêt à prendre en compte le PMSI psychiatrique qui devrait faire son apparition courant 2005. Une charte d'utilisation de l'informatique et de l'intranet-internet est en cours de réalisation. En revanche, à l'Assitance-Publique-Hôpitaux-de-Marseille, le système d'information actuel est bien insuffisant au regard des besoins de l'institution : les applications ne permettent pas d'accompagner le suivi du patient et le pilotage de la structure, la couverture institutionnelle est insuffisante et ne favorise pas la continuité et le partage des informations, l'architecture technique du SI est inadaptée. Comme il est précisé dans le projet d'établissement 2004-2009, « son évolutivité, son interopérabilité et sa sécurité ne sont pas garanties (…)», le système d'information hospitalier doit évoluer vers un système centré «patient » interopérable dans un délai de 3 à 5 ans ». « Le nouveau système sera centré vers le patient et sa sécurité sera particulièrement renforcée pour garantir la confidentialité des données médicales ».[46]

B) Un système d'information médical actuellement sous-informatisé

a) Un système fondé sur l'écrit et l'oralité

La pratique informatique étant longtemps restée éloignée de la pratique médicale, le système d'information médical reste, comme dans nombre d'établissements, sous-développé. Les données cliniques, diagnostiques ou encore thérapeutiques sont transmises de manière orale et par écrit, via le fax le plus souvent, l'échange d'informations entre médecins sur l'état du patient étant au cœur de la pratique médicale. Les données médicales sont donc essentiellement conservées dans des dossiers papiers, répartis entre les unités fonctionnelles. Il n'existe aucune source d'information complète sur les patients.

Au sein des services, chaque utilisateur doit donner son nom et son mot de passe, les autorisations d'accès étant déterminées par le groupe d'appartenance (médecin traitant, médecin somaticien, secrétaire médicale…).

b) Le choix d'un environnement non communicant : le « poste à poste »

Seuls les secrétariats médicaux sont informatisés (à l'exception de quelques cadres et médecins) et ne sont reliés entre eux que par …disquette. Les secrétaires

[46] Projet d'établissement consultable en ligne : http://www.ap-hm.fr/contenu/actualite/pdfs/00-Projet_Etablissement.pdf

médicales travaillent dans un même bureau fonctionnent en environnement *workgroup*[47], c'est-à-dire de poste à poste. Les *workgroups* définissent simplement l'appartenance du poste client à un service et ne gèrent pas la sécurité.

Chaque poste de travail peut être considéré comme un «domaine» où sont définis les utilisateurs, les mots de passe, les stratégies de sécurité locale, les partages et accès aux ressources. Cette gestion est très contraignante car elle requiert une intervention locale à chaque nouvelle modification (changement d'utilisateur, changement de mot de passe, partage, accès aux ressources, modification de la stratégie de sécurité locale etc.). Seule la sécurité définie localement sur le poste de travail interdira ou autorisera la communication avec une autre station ; elle est traitée de façon isolée sous la supervision du médecin-DIM. Ce système ne permet pas une gestion centralisée du contrôle d'administration, des comptes utilisateurs, de l'accès aux ressources, de la sécurité et de la configuration de la station de travail, de l'audit des événements (connexion, accès aux ressources, machines etc.). Selon l'administrateur réseau, «l'expérimentation d'un mini réseau entre deux services il y a quelques années a échoué car des données d'un service ont transité vers l'autre sans barrières. L'erreur a été de donner des modems à qui le demandait, or on n'a aujourd'hui qu'une approximation du nombre de modems et de portables avec modems intégrés en circulation. Bref, on a affaire à de l'informatique domestique, qui s'apparente à du bricolage »[48].

Il n'y a donc, à ce jour, pas ou peu de documentation sur les stratégies retenues et la gestion des sécurités d'accès (droits d'utilisateurs) pour répondre aux exigences de traçabilité et de contrôle ; de même qu'il n'existe pas ou peu de procédures dédiées à la gestion opérationnelle de la sécurité.

c) Une gestion informatisée orientée vers la production d'activité

Depuis 1989, les secteurs de psychiatrie publique sont astreints à fournir des statistiques d'activité (les fiches mensuelles et le rapport annuel de secteur à la Direction Générale de la Santé). Selon la présidente de la Commission Médicale d'Etablissement (CME), le CH Montperrin a institué une « procédure très rigoureuse, connue comme telle par l'ARH qui sait que les données émanant de Montperrin sont fiables ». Ces relevés, sans incidence économique directe pour les services, ne sont qu'un reflet partiel voire réducteur de la charge du travail et de l'activité. Par ailleurs, la loi du 31 juillet 1991 fait obligation aux hôpitaux de mettre en œuvre des systèmes d'information tenant compte

[47] Un *Workgroup* est un ensemble d'ordinateurs regroupés pour une fonction commune telle que partager les ressources au sein d'un même bureau comprenant un nombre très limité de stations de travail très rapprochées. En l'occurrence, deux stations de travail fonctionnent en workgroup dans chaque secrétariat médical.
[48] Entretien en date du 27 juillet 2004.

des pathologies, afin d'améliorer la connaissance de l'activité et des coûts et de favoriser l'optimisation de l'offre de soins[49].

Le système d'information médical regroupe les différents systèmes d'information des 14 secteurs médicaux du CH. Le logiciel de gestion des dossiers médicaux et de la fiche patient choisi par l'établissement permet essentiellement de saisir l'activité et d'élaborer un rapport d'activité conforme aux règles nationales. Le logiciel est implanté dans le secrétariat médical de chaque secteur et utilisé essentiellement pour sa fonction fiche patient. Les informations médicales soumises à l'obligation de transmission aux autorités de tutelle sont enregistrées manuellement par une secrétaire médicale de chaque secteur et transmises par disquette au statisticien de la SMTEIM[50] et au DIM qui les anonyment et les agrègent une fois par mois dans la base de données médicales afin d'élaborer des rapports d'activité portant, par exemple, sur le dénombrement des patients par âge et par sexe, sur le nombre de prises en charge à temps complet, à temps partiel, prise en charge ambulatoire, etc. Le risque de perte de temps et d'erreur est accru par cette procédure de ressaisie et le serveur actuel de la SMTEIM fait office de bibliothèque, stockant les programmes et les fichiers de données des utilisateurs, mais aussi de poste de travail pour le statisticien, faiblesses relevées par le rapport d'audit que nous présenterons ultérieurement. Il est à noter à ce titre que 48 % des utilisateurs du SIM ne savent pas si les données médicales informatisées sont bien protégées et que 14 % se prononcent négativement[51].

La question de l'implantation d'un réseau informatique physique est récurrente dans l'établissement depuis dix ans. Sur ce projet de réseau, la présidente du Collège de l'Information Médicale[52] (CIM) nous assure que les médecins sont favorables au principe pour autant « qu'il soit encadré par des limites que recommande l'éthique médicale »[53]. Pendant près de dix ans, il est pourtant resté une « Arlésienne ». La présidente du CIM souligne que le futur réseau devra être également extra-hospitalier, car sur une file active de 15000 personnes, seules 3000 sont hospitalisées en intra-hospitalier.

Le degré actuel d'informatisation ne permet pas de répondre aux objectifs, désormais assignés à l'informatique de santé, d'aide à la décision médicale, de formation continue, d'échange entre professionnels et avec les autorités et organismes chargés de la santé publique, de collecte des données médicales individuelles (dossier du patient) et

---

[49] Article L. 710-5.
[50] Structure Médico-Technique de l'Evaluation et de l'Information Médicales, organisme d'exécution des décisions du CIM, qui est l'instance politique.
[51] *Cf*. annexe I.
[52] Le CIM a remplacé le Département de l'Information Médicale à Montperrin, il y a environ sept ans. Structure politique et décisionnelle, il est doté d'une figure « politique », la présidente, d'une figure technique, le DIM, du statisticien de la SMTEIM et d'autres praticiens hospitaliers (les référents informatiques de chaque unité fonctionnelle « information médicale », chaque service étant doté d'une unité fonctionnelle « standard » à vocation budgétaire et d'une unité fonctionnelle information médicale qui se surajoute). Il a institué un règlement intérieur relatif à la décentralisation de l'information médicale et se réunit une fois par mois.
[53] Entretien en date du 06 septembre 2004

collectives (état de santé d'une population, évolution d'une pathologie, épidémiologie, morbidité), de gestion du risque et de la maîtrise des dépenses de santé, d'harmonisation dans la tenue des dossiers des patients. Pourtant, d'aucuns s'accordent sur la nécessité de mettre en œuvre des systèmes d'information médicaux intégrés, construits autour d'un dossier patient qui assure l'archivage, le partage et la traçabilité des données.

1.2 Définition de l'architecture-cible que la politique de sécurité informatique a vocation à couvrir

1.2.1 Les priorités retenues par le projet d'établissement dans le cadre du déploiement du système informatique médico-administratif

Il est encore difficile d'avoir une perception claire de l'architecture cible, car celle-ci nécessiterait une meilleure expression des besoins à couvrir et des objectifs. Néanmoins, à partir des éléments qui ont été portés à notre connaissance, nous avons tenté d'en dégager les grands contours, de trouver un biais pour cerner les besoins, la politique de sécurit devant s'appuyer sur ces derniers pour cohérente. L'objectif est de mettre à la disposition de l'établissement un système d'information ouvert et communicant, centré à terme sur la prise en charge du patient et couvrant l'ensemble des domaines fonctionnels de l'hôpital : gestion administrative des patients, gestion des ressources humaines, gestion économique et financière, gestion des fonction logistiques, mais aussi production des soins et activités médico-techniques. Il s'agit de répondre aux priorités du projet d'établissement, aux enjeux (comme le PMSI psychiatrique, voire une éventuelle tarification à l'activité) et aux contraintes légales et réglementaires. Cela implique d'instituer une politique de sécurité globale servant de référence obligée pour toute évolution du système d'information, que ce soit pour l'intégration d'un nouvel élément dans le système, pour la modification d'un élément existant ou pour l'interconnexion avec un système d'information partenaire. Or cette référence obligée va se heurter à la résistance du corps médical, qui au nom de la confidentialité, réfrène le partage des informations médicales.

A) Développer et structurer l'informatique médicale

L'objectif est d'améliorer la qualité des prestations, d'automatiser les tâches répétitives ou à faible valeur ajoutée, de faire gagner du temps aux soignants, d'optimiser la gestion des ressources humaines, de mettre en place des outils de pilotage médico-économiques et enfin de devancer les exigences des tutelles (CCAM, Comptabilité analytique, T2A).

a) L'informatisation des unités de soins, « Cheval de Troie » du système d'information cible

S'il « est tout de même étrange d'avoir d'abord informatisé en dehors du corps du métier qu'est le soin » comme le souligne le Directeur des soins[54], il faut reconnaître que les problématiques liées à la sécurité et à la confidentialité des données du patient ont longtemps constitué un frein à la mise en place et au développement du processus d'informatisation des soins. Profitant de la dynamique créée par le renouvellement des applications informatiques en 2003, le CH Montperrin a entamé en 2004 une vaste entreprise d'informatisation des unités de soins intra-hospitalières, conçue dans un premier temps pour délocaliser la gestion des plannings dans les unités, et à terme pour « mieux gérer les prescriptions thérapeutiques d'examens complémentaires et de médicaments, de vérifier leur bonne exécution »[55] et donc de répondre à deux grands objectifs : l'amélioration de la qualité et de la sécurité des soins et l'optimisation de la consommation des ressources. Une fois l'ensemble des unités de soins couvert par le réseau, il n'y aura plus d'obstacles « techniques » à une future informatisation du circuit du médicament[56]. Mais la réalisation de cette dernière est liée à l'état d'avancement de la mise en œuvre du dossier médical informatisé, qui n'en est qu'au stade de la réflexion. Quoi qu'il en soit, il sera d'autant plus difficile pour le corps médical de repousser indéfiniment la prescription informatisée, afin d'éviter la gestion d'un double circuit papier et informatique à la pharmacie, qu'un logiciel pharmaceutique d'aide à la prescription médicamenteuse, informant sur le bon usage du médicament, sécurisera l'administration par les soignants.

L'informatisation de unités de soins devrait permettre de réduire le nombre des niveaux de gestion et des échelons hiérarchiques et d'augmenter corrélativement les responsabilités des soignants. Une des conséquences pourrait être, à terme, la suppression du cadre intermédiaire puisque le cadre supérieur de santé détiendra davantage d'informations pour superviser un grand nombre d'agents investis d'une autorité décisionnelle supérieure. Cette démarche pourrait finalement transformer la structure hiérarchique de la prise de décision en réduisant le temps de recherche de l'information, en simplifiant le circuit, en assurant une traçabilité fiable et en élargissant la diffusion des informations.

L'interconnexion en réseau favorisera enfin le travail en équipe et la collaboration entre l'intra et l'extrahospitalier –ce dernier devant être informatisé et mis en réseau d'ici

[54] Entretien en date du 10 août 2004.
[55] Entretien avec un Cadre Supérieur de Santé, en date du 11 août 2004.
[56] Si la pharmacie est informatisée depuis longtemps et a développé depuis quelques années le principe de dispensation nominative des médicaments, la prescription continue d'être faxée.

cinq ans, et permettra de gommer l'éloignement géographique. Il faudra d'une part former les personnels médico-soignants en matière de technique informatique, revoir les organisations dans les bureaux et sur les lieux de travail et enfin modifier la présentation formelle de l'information. L'informatisation exigera, d'une part, une restructuration plus générale de l'organisation dans le sens d'un assouplissement et d'une décentralisation et, d'autre part, une nouvelle architecture du traitement de l'information.

b) La création d'un « monde » médical

Les services informatiques du CH Montperrin viennent de terminer la maquette du futur « monde médical » qui sera en réalité médico-soignant. Il sera créé dans un domaine *Active Directory*, distinct de l'administratif, lequel permet, par rapport aux *workgroups*, de gérer et d'administrer à partir d'un point unique les droits d'accès, la stratégie de sécurité du domaine[57], la stratégie de sécurité locale[58], l'audit des événements de connexion et d'accès aux objets et les profils des utilisateurs. Enfin et surtout, œtte solution apporte une plus grande sécurité des données (confidentialité, sauvegardes, etc.).

Il aurait été difficile de créer le « monde médical » dans le domaine administratif, les utilisateurs devant ouvrir une session sur le monde « administratif » au démarrage. Cela aurait généré des tensions d'ordre « politique », notamment avec les médecins chefs de service qui entretiennent une relation très paternaliste avec le personnel soignant et acceptent encore difficilement le transfert au directeur[59] de l'autorité hiérarchique sur le personnel infirmier.

Par ailleurs, les médecins n'accepteront ce monde médico-soignant que pour autant que l'informaticien qui sera en charge de ce dernier soit sous la responsabilité hiérarchique du corps médical et en particulier du médecin-DIM. La raison invoquée est de nouveau le caractère confidentiel des données médicales. Or cet informaticien serait tout aussi bien soumis au secret professionnel sous la responsabilité de la DSIO. Derrière cette exigence, nous décelons un manque de confiance de la part du corps médical vis-à-vis de l'administration. Dans une réunion du CIM en date du 30 août 2004, la Direction a confirmé qu'elle ne voyait aucun inconvénient à ce que l'informaticien travaille aux côtés du médecin-DIM, pour autant qu'il soit placé sous la responsabilité hiérarchique de la

[57] Tels que les mots de passe (renouvellement, complexité, longueur), le verrouillage des comptes, la connexion autorisée sur horaires définis,…
[58] Tels que le verrouillage des disquettes et CD, l'interdiction d'installation de programme, le verrouillage des sessions.
[59] Nous en prenons pour preuve la parution sur le site de la SMTEIM d'une annonce générale relative aux postes vacants d'infirmiers ou encore d'éducateurs au sein du CH Montperrin, postes pour lesquels il est possible de postuler en cliquant sur un lien correspondant à l'adresse e-mail du Directeur des soins ou encore d'un cadre de santé qui sont installés sur un domaine rattaché au Collège de l'information médicale et non pas à la Direction des Ressources Humaines ou à la Direction des soins. Du reste, le Directeur des soins ignore jusqu'à l'existence de cette adresse qui lui appartient pourtant.

Direction (du système d'information, des ressources humaines, ou encore des soins, la question n'étant pas tranchée).

Le domaine « médical » ne pourra être totalement indépendant car les utilisateurs médecins et soignants bénéficieront du service de messagerie interne du CH Montperrin dédié actuellement au système d'information administratif. Pour empêcher un utilisateur du domaine médical de s'authentifier sur le domaine « administratif » et inversement, une politique de mot de passe complexe (8 caractères minimum contre 4 actuellement) sera mise en place dans les deux domaines. Une stratégie de sécurité du domaine forte et contraignante est d'ores et déjà préétablie : le domaine médical bénéficiera des mises à jour antivirales automatiques et des mises à jour des failles critiques de sécurité du système équivalent au domaine « administratif ». Les postes de travail ne disposeront ni de lecteur de disquette ni de lecteur de Cdrom. Les ports USB seront désactivés. L'utilisateur sera totalement « verrouillé » au niveau de la station de travail et n'aura accès qu'aux applications autorisées. Par cette stratégie de sécurité locale, la station de travail s'apparente à un « client léger »[60], comme c'est le cas par exemple dans les Hôpitaux du Léman ou encore au CH E. Toulouse, avec un système d'exploitation local en plus, mais totalement transparent pour l'utilisateur. Il aurait pu être créé un seul domaine hébergeant les mondes administratif et médical, de manière totalement étanche, mais les stratégies de sécurité locale et de domaine n'auraient pas été indépendantes.

Mais l'objectif reste, à terme, la création d'un SI interconnecté et intégré, complètement sécurisé et garantissant la disponibilité, l'intégrité et la confidentialité des données.

c) Le système d'information cible : médico-administratif

L'objectif final du SDSI est d'assurer, à terme, la convergence entre les informatiques administratives et médicales dans une orientation plaçant le patient au cœur du système d'information et permettant sa gestion unique tout en assurant une efficacité maximum des ressources tant humaines que financières investies par l'établissement, mais également l'échange et le partage des données de santé informatisées, l'amélioration de la qualité des soins et de l'efficience de la structure hospitalière, la coordination et la continuité des soins. A court terme sont concernés par le projet les personnels administratifs, les directions fonctionnelles du CH – la DSIO en particulier –, le personnel soignant dont les cadres de santé, les secrétaires médicales et les médecins travaillant en intra-hospitalier. A moyen terme, il sera étendu à tout utilisateur du futur SII intégré, y compris en extra-hospitalier.

[60] Sorte de boîtier terminal connecté au réseau et relié à un écran, un clavier et une souris.

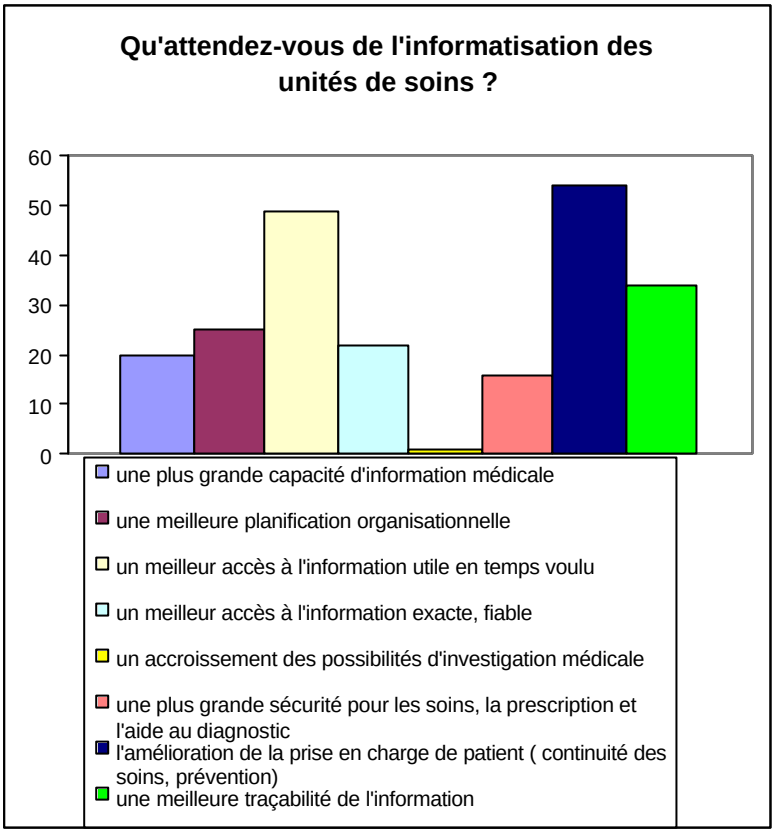
La réalisation de ces objectifs suppose un partage d'information et une interopérabilité des outils informatiques. Le futur système d'information cible devra dès lors concentrer des données médico-administratives dans des fichiers informatiques auxquels un grand nombre de personnes et de groupes externes pourront avoir accès, tout en assurant l'imperméabilité entre les données médicales et les données administratives. Dès lors, ces données seront encore plus particulièrement exposées au risque de destruction, d'usage frauduleux ou encore abusif ainsi qu'aux erreurs de traitement. Il s'agira de relier les différents professionnels de santé, l'intra et l'extra hospitalier, afin de palier les limites de l'exercice isolé, d'assurer une prise en charge globale du patient et de garantir la continuité des soins tout en respectant les contraintes budgétaires, car il convient aujourd'hui plus que jamais de maîtriser les coûts des systèmes et d'en piloter le fonctionnement.

A terme, le SIH couvrira deux domaines fonctionnels : administratif et médico-soignant. Il sera conçu comme un socle commun et consistera à :

- collecter et traiter de manière sécurisée les données utiles à l'activité de chaque service
- valider les données communes et nécessaires à la gestion des dossiers patients
- restituer l'information immédiatement ou de façon différée sous réserve de vérification de leur habilitation
- rechercher une plus grande sécurité pour les soins, la prescription et l'aide au diagnostic.

Les bénéfices attendus par les futurs utilisateurs du SI médico-administratif informatisé, questionnés sur ce sujet, sont les suivants : l'amélioration de la prise en charge du patient, un meilleur accès à l'information exacte, fiable[61], une meilleure traçabilité de l'information.

[61] Ce qui renvoie aux schémas relatifs au respect de l'intégrité et de la disponibilité, voir infra.



Nous y voyons également une possibilité d'accroissement des possibilités d'investigation médicale, participant en cela de l'amélioration de la prise en charge du patient en termes de qualité, de continuité des soins et de prévention. Ce système cible encouragera et facilitera la coopération entre les professionnels de santé qui expriment de plus en plus leurs besoins an matière de partage et d'échange d'informations. Il assurera une plus grande rapidité d'accès à l'information, ce qui est un avantage en particulier dans les structures extra-hospitalières (Centres-Médico-Psychologiques (CMP) en particulier). En définitive, il permettra de connaître, piloter, suivre et évaluer à la fois la production et la réception des soins, ainsi que la chaîne complexe des actes qui y concourent. Le système d'information médical informatisé devra fonctionner 24 H sur 24 et intégrer les notions particulièrement fondamentales dans ce domaine que sont la disponibilité, l'intégrité et la confidentialité.

Le contenu du logiciel de gestion des dossiers médicaux en psychiatrie, qui correspond à une gestion de la fiche patient, devra être amélioré par l'achat d'une nouvelle version et devra être concilié avec l'informatisation du circuit du médicament et celle du futur dossier médical partagé.

« L'architecture est prête depuis quatre ans », nous précise l'administrateur réseau, « le blocage n'est donc pas technique mais culturel et politique ». C'est également ce que relèvent M. FIESCHI et Y. MERLIERE ; « L'obstacle au changement

culturel que représente le partage de données des malades n'est pas seulement un problème technique »[62].

B) Garantir la sécurisation et la gestion des données médicales informatisées

a) Une condition sine qua non *de la future mise en place du Dossier Médical Personnel (DMP)[63] informatisé*

Parmi les futurs outils de coordination rendus possibles par le SII figure le dossier médical « virtuel » ou partagé. L'informatique et les nouvelles technologies de l'information et de la communication sont amenées à jouer un rôle clé dans l'avenir du dossier médical. Consciente de ce rôle, la DSIO souhaite s'orienter d'ici 5 ans vers la construction d'un dossier médical informatisé qui soit le résultat d'une collecte de données générées depuis chaque point en intra et en extra hospitalier. Là encore faudra-t-il s'assurer que les impératifs sécuritaires, qui assurent la cohérence et la fiabilité et la confidentialité des informations en matière de données médicales informatisées, soient garantis.

Les dossiers médicaux des patients sont répartis entre les hôpitaux, les cabinets médicaux, les pharmacies, les laboratoires etc., et ne sont accessibles que chez le fournisseur de soins qui les a créés. Le regroupement de l'ensemble de ces données en un seul DMP informatisé pose la question de la sécurité du stockage et de la transmission des informations médicales dont il faut garantir la confidentialité[64].

Le futur « dossier médical (médico-soignant) partagé », qui sera obligatoire pour tous les Français de plus de 16 ans à partir de 2007[65], devra assurer une identification fiable du dossier patient au sein du SIH (indexer les éléments du dossier patient). Les établissements de santé, les professionnels libéraux déposeront, selon la note d'orientation sur les données du patient partagées[66] remise au ministre par le Professeur M. FIESCHI, à une « adresse qualité santé » placée dans un « coffre-fort », de chaque patient, chez un hébergeur agréé[67], les informations dont ils disposent sur leurs patients. Dans son récent rapport annuel, la CNIL exige que des normes strictes de sécurité soient

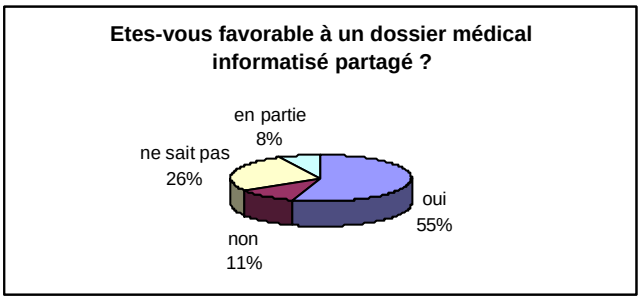
---

[62] *Les données du patient partagées*, *op. cit.*, p. 14.
[63] *Cf.* article 3 de la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie : « Afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé, chaque bénéficiaire de l'assurance maladie dispose, dans les conditions et sous les garanties prévues à l'article L. 1111-8 du code de la santé publique et dans le respect du secret médical, d'un dossier médical personnel constitué de l'ensemble des données mentionnées à l'article L. 1111-8 du même code, notamment des informations qui permettent le suivi des actes et prestations de soins ».
[64] La loi du 4 mars 2002 (*op. cit.)* cherche à garantir la confidentialité des informations médicales (et non pas de toutes les informations) conservée informatiquement ou transmises électroniquement, *cf.* article L. 1110-4, al 4.
[65] Tel que l'a annoncé en 2004 l'actuel ministre de la santé, Philippe DOUSTE-BLAZY, sur la base des principes suivants : consultation sur accord du patient, usage de la carte vitale dernière version et de la carte de professionnel de santé du médecin, agrément d'un site hébergeur hautement sécurisé, performance des systèmes d'information des hôpitaux, cliniques privées et cabinets de ville performants.
[66] *Les données du patient partagées partagées*, *op. cit.*
[67] Un décret en préparation prévoit leur contrôle et leur labellisation par les pouvoirs publics.

imposées aux hébergeurs de données, lesquels devront être agréés par décret en Conseil d'Etat[68].

Le CH Montperrin n'a aucune expérience en ce qui concerne l'informatisation des dossiers des patients au niveau de l'ensemble des services. Néanmoins, ce dossier est d'ores et déjà conçu par une cellule multidisciplinaire de réflexion sous son aspect technique (une configuration limitée à un secteur/service qui permet une mise en réseau de l'ensemble des secteurs avec tous les verrous nécessaires), et sous son aspect « contenu » proprement dit qui est en phase d'achèvement.

Le DMP ne devra contenir, selon les médecins interrogés, que des comptes-rendus synthétiques d'entretien (médical, infirmier, avec les familles), des fiches de liaison ainsi que des données sur les aspects somatiques de nature à objectiver la pathologie. Ils ont choisi une phase intermédiaire dans la réalisation d'un dossier médical papier « informatisable ». Interrogés sur la future mise en place du DMP, plus de la moitié des utilisateurs du SIM se disent favorables à ce dernier :



Pourtant, lors des entretiens non directifs, la majorité des médecins, dont la présidente du CIM, redoutent que le futur DMP serve de mouchard ou cache un « big brother » et craignent à ce titre que la confidentialité des données, garantie par la loi Kouchner[69] relative aux droits des malades, ne soit bafouée. Ils doutent par ailleurs qu'il puisse être généralisé « au plus tard avant le 1er juillet 2007 », comme le prévoit la loi. Au contraire, au CH Valvert, dès 1997, la demande prioritaire provenant du corps médical concernait la mise en place d'un dossier médical informatisé et sécurisé, incluant la prescription médicamenteuse et à partir duquel serait généré le PMSI.

b) L'utilisation, à terme, de la Carte Professionnelle de Santé (CPS) : vecteur de responsabilisation

[68] *Cf.* annexe II : le cadre est précisé par la loi du 4 mars 2002 et la récente loi sur l'assurance maladie (2004-810, *op. cit.*) qui prévoient que les données de santé recueillies peuvent être déposées par les professionnels de santé, les établissements ou les patients auprès d'une personne physique ou morale agréée. L'hébergement des données ainsi que les modalités d'accès et de transmission doivent être subordonnées à l'accord de la personne concernée mentionné dans le contrat d'hébergement. Les hébergeurs sont évidemment soumis au secret professionnel.
[69] Loi n°2002-2003, *op. cit.*

La Commission Nationale Informatique et Libertés (CNIL)[70] encourage vivement le chiffrement, le cryptage et surtout l'utilisation de la CPS qui devrait permettre d'assurer la sécurité nécessaire à l'identification du médecin, en tant qu'elle est le passeport essentiel à la généralisation des échanges informatiques dans le monde de la santé. Mais la CPS ne résoudra pas le problème culturel du partage des données du dossier hospitalier.

Avec l'informatisation des services, l'utilisation de la CPS devra être posée au travers d'une formation collective et individuelle, comme ce fut le cas aux HUS, établissement hautement avancé en matière de système d'information informatisé et travaillant à la sécurisation depuis dix ans, sur la notion de confidentialité, à l'attention du personnel médical mais aussi soignant. Comme a pu le souligner le DIM de ce CHU, « la confidentialité des données, au sens de la préservation de l'intimité des personnes, est présente en bonne place dans chacun de nos projets, de manière à permettre de manière simple aux utilisateurs tous les accès légitimes dont ils ont besoin pour travailler, mais à les limiter aux seuls accès légitimes ».[71]

L'avantage sera évidemment le « zéro papier », une responsabilisation accrue des acteurs et une amélioration des pratiques de confidentialité.

c) La file active aujourd'hui, le PMSI psychiatrique et la tarification à l'activité demain ?

Bien que les CH psychiatriques ne soient pas concernés par l'actuelle tarification à l'activité (*cf*. plan Hôpital 2007 lancé en novembre 2002) et restent financés selon le modèle de ressources actuel, la lame de fond devrait déferler dans les années à venir sur la psychiatrie. Le système d'information devra dès lors être suffisamment performant pour accueillir, à terme, le PMSI, voire une tarification à l'activité psychiatrique.

« Dans les services hospitaliers, c'est le lancement au milieu des années 80 du programme de PMSI qui a été le révélateur de la nécessité pour les médecins d'utiliser les ressources de l'informatique », note F. PONCHON[72]. Dans le prolongement de la mise en place du PMSI dans les établissements de Médecine-Chirurgie-Obstétrique (MCO) en 1995 et dans les établissements de Soins de Suite et de Réadaptation (SSR)) en 1998, des groupes de réflexion coordonnés par la DHOS – dont la mission PMSI en particulier – travaillent depuis plusieurs années à la définition d'un programme de médicalisation des systèmes d'information (PMSI) adapté à l'activité psychiatrique. Après une étude de faisabilité réalisée entre 1990 et 1994 et la constitution d'une base de données entre 1995

[70] Instituée par la Loi 78-17 du 6 janvier 1978, dite loi Informatique et Libertés, elle est chargée d'appliquer dans le domaine informatique les limites légales prévues pour la protection des individus.
[71] Entretien électronique en date du 6 mai 2004
[72] PONCHON F., *Le secret professionnel et l'information du malade*, éd. Berger-Lévrault, 1998, p. 106.

et 1998, janvier 2002 marque le début de l'expérimentation[73] en psychiatrie pour quelques régions pilotes (Rhône-Alpes, Aquitaine, Lorraine, Ile de la Réunion, et partiellement l'Ile de France), ainsi que pour les établissements volontaires situés en dehors de ces régions[74]. L'objectif est la généralisation du recueil de l'activité externe au 1er janvier 2005, et une généralisation globale à partir du 1er juillet 2005. Tous les établissements ayant une activité de psychiatrie générale ou de psychiatrie infanto-juvénile sont concernés qu'ils soient publics, privés ou privés participant au service public. Or, à ce jour, il n'est pas certain que ce calendrier soit respecté pour de multiples de raisons. Le retard du PMSI en psychiatrie s'explique, selon les médecins interrogés, par son inadéquation à la spécialité : « le PMSI a été imposé aux professionnels, il est tellement lourd que c'est infaisable (…) On n'en tire aucune donnée valide ; les DIM qui l'expérimentent sont obligés de « bricoler », nous confie la vice-présidente de la conférence des présidents de CME de CHS, M.T. LORIANT, qui fait partie du groupe de pilotage sur le PMSI psychiatrique[75]. Réaliste, elle ajoute : « le groupe veut que la psychiatrie entre dans la T2A[76] car il a conscience que ce serait suicidaire de rester en dehors. Pour l'heure, il réclame une allocation pluraliste qui tienne compte des coûts par structure et un recueil allégé ». Quand au médecin-DIM du CH Montperrin, il n'hésite pas à s'attribuer cet échec. Il faisait en effet partie du « groupe des 13 »[77] au début des années 90, qui travaillait au côté du ministère sur l'expérimentation du PMSI dans une centaine de structures. Selon lui, « les items retenus et imposés par le ministère étaient déconnectés de la psychiatrie car trop subjectifs et quantitatifs. Comment voulez-vous coter la durée d'un entretien ? En 98, les résultats sont tombés ; bien que les hypothèses formulées n'étaient pas valides sur le plan médico-économique, le ministère a souhaité maintenir ce programme ». Il ajoute qu'il s'est alors retiré du groupe, soutenu en cela par l'opposition syndicale et que finalement « le Ministère a fait marche arrière ». G. MOSNIER pense quant à lui qu' « on a trop laissé les rennes au DIM, au groupe des treize (…) Le PMSI et trop lié à la MCO et pas assez adapté à la psychiatrie, or cette dernière est en situation très inconfortable en l'absence de modèle d'allocation budgétaire spécifique (…). La psychiatrie ne refuse pas l'auto-évaluation pourvu qu'elle sa fasse de manière adéquate », c'est d'ailleurs la raison pour laquelle la notion actuelle de « trajectoires de santé » est mieux accueillie parmi le corps médical.

---

[73] *Cf*. Circulaire DHOS/E3/2001/n° 625 du 19 décembre 2001 relative à la mise en oeuvre du PMSI-psychiatrie, à titre expérimental.

[74] L'expérimentation du PMSI en psychiatrie a permis de mettre en place dans près de 180 établissements un système d'information médicalisé. Elle se fonde sur une classification en Groupes Homogènes de Journées (GHJ) et Groupes Homogènes d'Actes (GHA).

[75] Entretien en date du 10 septembre 2004.

[76] dont le processus de généralisation a été initié en janvier 2004 pour le financement des établissements ayant une activité en médecine, chirurgie, obstétrique, tarification qui doit être étendue, dans un avenir proche, aux soins de suite et de réadaptation.

Comment dès lors le PMSI pourrait-il être perçu par le corps médical comme une « immense chance à saisir pour la Santé mentale »[78] ?

Selon Jeanne BOSSI, Chef de division des affaires publiques et sociales à la CNIL, «le champ d'application n'est pas aussi clair que pour la MCO. Le statu quo demeurera en matière de PMSI psychiatrique tant qu'il ne sera pas modifié dans sa finalité (…) Le problème, c'est que les psychiatres veulent anonymer complètement les données à la source et non à partir du DIM comme en MCO, ce qui est difficile à comprendre car le médecin-DIM est le garant de la confidentialité. Par ailleurs ils sont également opposés à l'indication de la pathologie psychiatrique, alors qu'il est possible de mettre en place des verrous de sécurité très forts ». Elle constate que les problèmes recensés lors de demandes d'avis[79] ou de déclarations[80] à la CNIL au travers des dossiers d'expérimentation du PMSI psychiatrique reposent essentiellement sur le respect du secret médical, «les psychiatres y sont en effet très sensibilisés et invoquent la spécificité de leur spécialité qui repose sur la confiance, le colloque singulier, ce qui rend l'évaluation plus difficile ». Il convient de noter que la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel [81] instaure désormais un seul et même régime pour les fichiers publics et privés, qui sont soumis à un contrôle a posteriori renforcé de la CNIL[82].

La mise en place opérationnelle du PMSI nécessitera une informatisation généralisée des unités de soins. Un réseau fédérateur supportant l'ensemble des données d'activité, sans ressaisie d'informations permettra au DIM de ressembler les données, de les synthétiser et de les exploiter de façon fiable.

Les membres du comité de pilotage du PMSI en psychiatrie estiment par ailleurs que la psychiatrie ne peut rester en dehors du mode de financement par tarification à l'activité. Il est aujourd'hui nécessaire de construire rapidement un outil de tarification à l'activité pour la psychiatrie, compte tenu du nouveau contexte de financement des établissements de santé. Il a été prévu que l'année 2004 serait consacrée au recueil des actes directs au patient pour tester à nouveau la classification en GHJ et en GHA, la pertinence de cette dernière en psychiatrie étant pour l'instant remise en question. Les

---

[77] En décembre 1990 a été mis en place un groupe de travail composé de psychiatres d'exercice public, désigné sous le terme "Groupe des Treize". Ce groupe était chargé par le Ministère de travailler sur la gestion de l'information médicale en psychiatrie.

[78] Comme le considérait un psychiatre, membre du groupe technique n°1 pour le PMSI en Santé Mentale, interviewé sur la question : WAGUENAAR G., Informatique médicale et PMSI, *Le journal de Nervure*, mai 2000, n°4.

[79] Article 1 de la loi Informatique et Libertés : demande particulière pour les personnes morales de droit public ou privé gérant un service public, qui porte sur le traitement et sur le « projet acte réglementaire » d'habilitation de l'utilisateur à exploiter ce traitement.

[80] Déclaration simplifiée pour tous les traitements pour lesquels la CNIL a édicté une norme (paie, autocommutateurs, etc.) et déclaration ordinaire (article 16) qui se présente comme une demande d'avis mais sans acte réglementaire.

[81] Loi n°2004-801 qui modifie la loi Informatique et Libertés du 6 janvier 1978.

[82] Jusque là, les fichiers publics et privés n'avaient pas le même régime : les fichiers publics devaient être autorisés et les fichiers privés déclarés. La CNIL effectuait donc un contrôle a priori des fichiers publics et un contrôle a posteriori des fichiers privés. Désormais, les fichiers créés par les pouvoirs publics relèvent du régime des fichiers privés. L'avis de la Commission sur la création d'un nouveau fichier ne sera donc plus que consultatif. .

travaux sur la classification des séquences de soins (trajectoires) seront poursuivis pendant l'année 2005. La perspective reste plurielle puisque le comité de pilotage souhaite des modes de financement diversifiés : lié à l'activité, lié aux charges fixes, lié aux missions d'intérêt général. Il sera proposé au Ministre de la santé une généralisation en deux temps. Au 1er janvier 2005, une généralisation de l'activité externe, au 1er juillet une généralisation globale, afin d'obtenir un recueil exhaustif des toutes les données d'activité à partir du 1er janvier 2006. Le SI devra conserver les informations nécessaires à la connaissance de l'activité et des populations prises en charge, à l'organisation des soins, à l'allocation budgétaire et aux futurs travaux sur une classification des séquences de soins[83]. Le futur PMSI, voire la future tarification à l'activité, requiert l'adaptation de l'informatisation et l'intégration d'outils de pilotage médico-économiques idoines. L'échec du PMSI psychiatrique, expérimenté depuis 2002, est attribué par les membres du CIM interrogés sur la question, à plusieurs facteurs : l'objectif initialement poursuivi fut de rationaliser pour rationaliser alors que la psychiatrie se prête difficilement à une évaluation médico-économique ; un même patient peut recevoir plusieurs diagnostic et un volume de soins variable selon la période envisagée ; une complexité terminologique et méthodologique. Il leur semble qu'un système « calé sur la fiche patient » serait plus adéquatement exploitable.

Selon E. DUSEHU, l'échec de l'expérimentation du PMSI psychiatrique réside dans la « volonté aveugle de caractériser les séjours, alors que la référence en psychiatrie est la file active (…) La psychiatrie se prête difficilement à une classification médico-économique ».

Par ailleurs, bien qu'il s'agisse d'une saisie de l'activité médicale en tant qu'activité génératrice de dépenses et de recettes, et non comme activité soignante, « Le PMSI permet à l'administratif de poser un regard très aigu , voire inquisiteur sur le médical (…). L'administratif va pouvoir exercer un contrôle de l'activité médicale donc renforcer son emprise sur les médecins… »[84].

La présidente de la CME, qui fait partie du COPIL sur le PMSI psychiatrique, n'imagine pas une installation définitive et opérationnelle avant 2007, pour autant « que l'outil soit reconstruit et change de nom ».

C) Des enjeux transversaux

Les enjeux liés à la mise en œuvre d'une politique de sécurité du système d'information ne doivent pas être réduits à un défi technologique mais doivent constituer

[83] Compte-rendu de la réunion du Comité de pilotage du PMSI en Psychiatrie, du 22 janvier 2004.
[84] Interview d'un chirurgien, J.M. AMAR, Où en est l'informatique hospitalière ? *Décision Santé*, mai 1997, n°113, p. 24.

la base d'une démarche progressive et construite dans le respect des contraintes suivantes : maîtrise de la qualité des soins, respect des contraintes légales et réglementaires, optimisation et rationalisation du traitement de l'information, maîtrise des aspects financiers et humains, pilotage concerté entre les acteurs.

La mise en place d'une politique de sécurité du système d'information trouve son origine dans la volonté politique de transformer structurellement le système d'information actuellement partiel pour le rendre plus performant. Le premier enjeu est donc économique, ou plutôt médico-économique, puisque les progrès des techniques réseau promettent de réduire les coûts liés au mouvement de grandes quantités de données et à leur accès. S'il ne doit pas être cantonné de façon simplificatrice à un centre de coûts (raccourci résultant du fait que les directions des finances et du système d'information sont le plus souvent réunies sous la responsabilité de la même autorité, que ce soit d'ailleurs au sein du monde hospitalier[85] ou des entreprises privées), le système d'information permet néanmoins une évaluation budgétaire des coûts et des charges, indissociable de toute planification pluriannuelle des actions élaborée par le schéma directeur.

Par ailleurs, on peut attendre du système d'information qu'il offre une meilleure connaissance de l'activité hospitalière, des besoins de santé, voire une maîtrise plus rationnelle des coûts (réduction de la durée des séjours, réduction de certaines tâches) à l'échelle des unités médico-techniques (évaluation d'activité), de l'établissement (planification financière et gestion des ressources) ou à l'échelle nationale (planification des dépenses hospitalières, épidémiologie et prévision des coûts).

Comme le souligne E DUSEHU[86], ancien membre du CNOM et membre de l'ANAES, les enjeux hospitaliers de l'informatique de santé sont caractérisés par une démarche centrée autour du patient avec une préoccupation médico-économique clairement affichée[87]. En dehors de l'entretien avec ce dernier, encore conseiller il y a deux ans et qui suit l'activité du CNOM de très près, nous n'avons pas obtenu de suite aux demandes répétées d'entretien formées à l'attention du CNOM. E. DUSEHU nous a confié ne pas en être surpris : « il n'y a plus de production nouvelle du CNOM depuis deux ans, l'Ordre ne fait plus sauter les fusibles ; il est devenu un édredon ».

Du côté médico-soignant, les principaux enjeux de l'harmonisation du système d'information, de son informatisation et de sa sécurisation, sont l'amélioration des

---

[85] *Cf*. les résultats de l'enquête sur la gestion des systèmes d'information dans les centres hospitaliers, réalisée sous l'égide du Collège des DSIO des Centres Hospitaliers, présentés en novembre 2003 au Forum national des DSIO, à l'ENSP.

[86] Médecin anesthésiste-réanimateur et ancien médecin DIM du CH de Compiègne, il accompagne depuis octobre 2003 la mise en place d'un dossier médical informatisé au CHU d'Amiens. Il fut membre du CNOM de 1981 à 2002, dont il est parti avec l'ancien président et deux autres conseillers « pour divergences éthiques majeures », nous confia-t-il lord de notre entretien en date du 6 août 2004. Il collabore aux travaux de l'ANAES depuis 1999, et est expert-visiteur depuis 2004.

[87] Lors du débat sur *Les enjeux de l'informatique de santé*, CNOM, 6ème jeudi de l'Ordre, Paris, février 2000. Disponible sur Internet : http://www.conseil-national.medecin.fr/?url=colloque/article.php&offset=5

pratiques cliniques par la mise en commun d'informations médicales dans des conditions optimales de sécurité et dans le respect de la confidentialité, ainsi que l'optimisation de l'organisation de la dispensation des soins. L'informatique concourt à assurer la qualité des soins en réduisant les délais de communication inter-services et l'échange d'informations entre équipes. Elle permet également d'améliorer les pratiques en fournissant aux professionnels de santé une aide en ligne (aide à la prescription, base de données etc.).

Enfin, dans le domaine des SI, on accorde en général plus d'attention à l'intégrité financière qu'aux considérations éthiques. Or, il est indispensable que la politique de sécurité couvre des questions telles que la reconnaissance des responsabilités inhérentes à l'usage des SI et la définition de normes de protection de la qualité du système assurant la sécurité au niveau des individus et de la société. D'autant plus que la modernisation du SI peut produire des changements sociaux profonds qui menacent la répartition actuelle du pouvoir, des droits et des obligations.

Ce qui nous conduit vers le dernier enjeu : l'enjeu social, le SI étant en lui-même un vecteur de progrès social et en même temps une arme dangereuse qui peut ébranler les valeurs sociales fondamentales.

Si les gestionnaires, les médecins et les soignants ont conscience de ces enjeux, il convient encore de les convaincre de l'importance de la modernisation de leur système d'information.

La connaissance de ces enjeux renforce la nécessité d'une construction simultanée et étroitement corrélée du schéma directeur et de la politique de sécurité, dont il convient de souligner les interactions : la politique de sécurité devra être en mesure de proposer au schéma le cadre et les objectifs à atteindre et le compléter sur les options possibles tandis que ce dernier devra proposer des solutions.

Avant de présenter l'élaboration de la politique de sécurité, il convient de s'intéresser à l'environnement normatif dans lequel cette dernière doit évoluer. Des normes et standards européens ont émergé au cours des dernières années pour permettre de sécuriser les échanges informatiques d'une manière fiable, homogène et interopérable.

1.2.2 La mise en conformité avec l'environnement normatif

L'hôpital, qui informatise les données administratives et héberge les dossiers médicaux, doit dès lors prendre toutes les mesures organisationnelles et techniques pour répondre aux obligations légales et réglementaires qui encadrent la sécurité des informations.

L'établissement doit se mettre en conformité avec les normes, bonnes pratiques et références relatives à l'adoption et la conception d'un SI sécurisé, respectant les droits du malade et le secret médical. Nous ne traiterons pas ici de la réglementation relative à la protection des logiciels, des régimes cryptographiques, des bases de données, à la signature électronique, mais nous aborderons de manière synthétique les grands principes qui régissent le traitement des données personnelles et médicales.

A) Les normes déontologiques et juridiques

a) La garantie du respect des droits de la personne et de la vie privée

En 1997, une délibération de la CNIL soulignait l'obligation d'adopter des procédures d'anonymation dans le traitement des données nominatives et attirait l'attention sur « la nécessité de prendre des mesures de sécurité appropriée ». La loi du 6 janvier 1978[88] impose à tout responsable de traitement une obligation de sécurité, qui se traduit par l'obligation de prendre toutes précautions utiles pour éviter la déformation, la divulgation ou l'utilisation détournée de données issues de prescriptions médicales, dès lors que ces données permettent d'identifier le patient. En pratique, il s'agit de mettre en place des mesures physiques et logiques (mots de passe etc.). Avec plus de six ans de retard, la France vient, le 6 août 2004[89], de mettre en conformité la loi du 6 janvier 1978, en transposant en droit interne la Directive européenne du 24 octobre 1995 sur la protection des données personnelles[90]. La loi Informatique et Libertés, version 2004, s'applique désormais aux traitements automatisés et non automatisés de *données à caractère personnel*[91] et non plus d'informations nominatives. Cette nouvelle terminologie plus large permet d'englober un plus grand nombre de situations. La loi de 78 modifiée énonce trois principes :

- la légitimité des applications et la pertinence des données[92] (adéquation entre données traitées et finalité poursuivie)

---

[88] Dans son article 29.

[89] Loi n° 2004-801, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *op. cit.*, *cf.* annexe II.

[90] Directive 95-46/ CE du Parlement européen, entrée en vigueur le 25 octobre 1998. En vertu de cette directive, les données doivent être traitées loyalement et licitement, collectées pour des finalités déterminées, explicites et légitimes. Elles doivent être adéquates, pertinentes, non excessives et exactes. La directive confère un droit d'information (article 10 et 11), un droit d'accès et de rectification, (article 12), un droit d'opposition (article 14). Le responsable du traitement a la charge d'assurer la confidentialité des données à caractère personnel et de mettre en œuvre les mesures techniques et d'organisation appropriées pour les protéger contre la destruction accidentelle ou illicite, la perte, l'altération, la diffusion ou l'accès non autorisés.

[91] *Cf.* l'article 2 nouveau de la loi 78-17 : « constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres », annexe II.

[92] *Cf.* article L 4113-7 du CSP et la délibération n°97-008 du 04 février 1997 portant adoption de la recommandation du 4 février 1997 sur le traitement des données personnelles de santé.

- la confidentialité des données et la sécurité des traitements (physique et logique)
- l'information et le respect des droits des personnes (droit à l'information préalable, droit à l'opposition, droit à l'oubli, droit d'accès et de rectification).

Les données à caractère personnel doivent être licites[93] et ne peuvent être collectées et traitées que pour des finalités déterminées et légitimes. La loi établit à la charge du responsable des traitements de données une présomption de responsabilité pour tout dommage du fait d'un traitement illicite de l'information, et ne prévoit l'exonération de sa responsabilité que s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable. Le responsable des traitements a l'obligation d'informer les personnes concernées, notamment lorsque les données les concernant ne sont pas recueillis directement auprès d'elles, l'identité du responsable du traitement, la finalité du traitement, le caractère obligatoire ou facultatif des réponses, les conséquences éventuelles d'un défaut de réponse, les destinataires des données. Il se doit de conserver les données et d'en préserver la sécurité sous peine de sanction. L'accent est mis sur le consentement de la personne concernée par la collecte et le traitement de ses données à caractère personnel[94]. Le droit d'opposition[95] est maintenu et sera désormais discrétionnaire et sans frais lorsque les données seront utilisées à des fins de prospection, notamment commerciale[96]. Enfin, la loi prévoit, sans changement, le droit d'accès[97] et à rectification des données à caractère personnel par les intéressés[98].

La loi du 6 août 2004 a également renforcé les pouvoirs de contrôle et de sanction[99] de la CNIL, l'article 44 en particulier qui autorise l'accès des membres de la CNIL aux locaux à usage professionnel[100] de 6 heures à 21 heures ainsi que la communication de tous documents nécessaires à leur investigation et leur accès aux programmes informatiques et aux données, sous le contrôle du TGI le cas échéant. « Le secret médical ne pourra pas être opposé lors du contrôle[101], en cas d'accès aux bases de données nominatives, car les membres de la CNIL sont astreints au secret professionnel » précise Jeanne BOSSI.

Comme le prévoit l'article 22, un correspondant du CNIL à la protection des données sera nommé dans l'établissement et chargé d'assurer de façon indépendante le

---

[93] C'est-à-dire collectées et traitées de manière loyale et licite, pour des finalités déterminées, être adéquates, pertinentes et non excessives face à leur finalité, être exactes, complètes et mises à jour et enfin être conservées en respectant les délais de conservations, *cf.* Chapitre 2 de la loi n°2004-801, en annexe II.
[94] Article 7 nouveau.
[95] La loi de 1978 subordonnait le droit d'opposition à la justification de « raisons légitimes ».
[96] Article 38 nouveau.
[97] Le droit d'accès donne à toute personne la possibilité de connaître l'existence ou non, dans un fichier, de données la concernant et, si elle le désire, d'en obtenir la communication. Cette dernière a par ailleurs accès à l'ensemble des informations concernant sa santé, informations détenues par les professionnels des établissements de santé et qui sont formalisées et contribuent à l'élaboration et au suivi du diagnostic et du traitement ou à une action de prévention (Article L.1111-7 inséré dans le Code de la santé publique par l'article 3 de la loi du 4 mars 2002 précitée).
[98] Article 40 nouveau.
[99] Administratives, financières (jusqu'à 150.000 euros, doublées en cas de récidive), pénales, *cf.* annexe II.
[100] Des secteurs privé et public.
[101] Qui peut être réalisé aux fins d'information ou dans le cadre d'une plainte.

respect des obligations prévues par la loi[102]. En contrepartie, l'établissement ne sera plus tenu de procéder aux déclarations préalables pour les fichiers peu sensibles, prévues par les articles 23 et 24. Jeanne BOSSI souligne que « son indépendance est essentielle. Il ne pourra pas être le chef d'établissement, ni soumis directement à son autorité hiérarchique ? La CNIL pourra lui retirer sa fonction en cas de besoin (…). Il sera une sorte de DIM bis qui ne pourra pas recevoir d'injonctions ».

La loi de transposition étant adoptée, le Décret d'application de la loi du 4 mars 2002 relatif à la politique de confidentialité devrait paraître à la fin de l'année.

Le corollaire de la protection des données personnelles est la protection de la vie privée[103] des individus dont les données personnelles font l'objet d'un traitement automatisé. « Le droit au secret de la vie privée (…), par extension au secret professionnel[104] en milieu hospitalier doit être regardé comme un des droits fondamentaux de la personne humaine ». [105]

Le CH Montperrin a jusqu'ici toujours satisfait à son obligation de déclaration préalable à la CNIL de tout traitement automatisé des données de santé[106]. Ses applications ont reçu l'aval de la CNIL et un protocole a été signé.

b) Traitement des données médicales et respect du secret médical

L'accès en ligne à des renseignements médicaux personnels soulève de graves questions sur la protection de la vie privée. Si des pirates informatiques peuvent s'infiltrer dans le site de l'hébergeur du DMP, ils pourront accéder à des dossiers protégés et briser la confidentialité. Or, les établissements sont tenus de protéger la confidentialité des informations qu'ils détiennent sur les personnes qu'ils accueillent. Selon le code de déontologie médicale, en vertu de l'article 73, le médecin doit protéger les documents médicaux, « quels que soient le contenu et le support de ces documents…contre toute indiscrétion », ce qui confère au patient un droit à la sécurité des informations qui le concernent. La CNIL recommande que les instances ordinales concernées soient consultées lors de la mise en place de fichiers d'informations médicales, en particulier, en

---

[102] Cette disposition nécessite un Décret en Conseil d'Etat pris après avis de la CNIL.

[103] Article L 1110-4 de la loi du 4 mars 2002 : « toute personne prise en charge par un professionnel, un établissement, un réseau… a droit au respect de sa vie privée et du secret des informations la concernant » ; charte du patient hospitalisé : « le respect de la vie privée est garanti à tout patient hospitalisé, ainsi que la confidentialité des informations personnelles, médicales et sociales le concernant », repris par l'article 2 de la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie (*cf*. annexe II). La protection, de la vie privée est également abordée par la Directive 2002/58/CE, dite Directive vie privée et communications électroniques, du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

[104] *Cf*. article 2, al. 3 de la loi du 13 août 2004 précitée : « Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé ainsi qu'à tous les professionnels intervenant dans le système de santé ».

[105] Phrase introductive de l'ouvrage de PONCHON F., *Le secret professionnel à l'hôpital et l'information du malade*, *op. cit.*

[106] Le secteur public hospitalier est soumis à une procédure de « demande d'avis », dès lors qu'est projeté la mise en place d'une application informatique touchant à un traitement automatisé des données de santé.

ce qui concerne les modalités de participation des professionnels de santé[107]. Les données médicales concernant les patients, même anonymées, ne peuvent être utilisées à des fins de promotion ou de prospection commerciale dès lors qu'elles sont associées à l'identification du professionnel de santé[108]. Les dossiers médicaux des patients doivent être conservés sous la responsabilité des médecins qui en assurent le suivi[109].

Conformément à la directive 95-46, les données médicales sont considérées comme « sensibles », lesquelles ne peuvent être traitées sans le consentement de la personne concernée[110]. Les données sensibles sont soumises au régime de l'autorisation, à l'exception des traitements mis en œuvre par les médecins ou les biologistes et nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements[111]. Les établissements de santé, publics ou privés ont l'obligation de communiquer aux personnes recevant ou ayant reçu des soins, sur leur demande, les informations médicales définies à l'article L.1111-7. Cette communication est effectuée, au choix de la personne concernée, directement ou par l'intermédiaire d'un médecin qu'elle désigne[112]. Toute personne peut faire corriger, compléter ou mettre à jour les erreurs qu'elle a pu déceler à l'occasion de la communication des informations la concernant. Elle peut également refuser de figurer dans certains fichiers ainsi que la communication, à des tiers, d'informations la concernant.

Le secret médical est quant à lui un principe très fort de la déontologie médicale, particulièrement en psychiatrie. Il est la transposition, pour les médecins, du secret professionnel et s'impose à tout agent intervenant dans le processus de soin (médecins, soignants, assistantes sociales, diététiciennes etc.)[113]. Ce secret est imposé, depuis la loi du 4 mars 2002, à tout professionnel de santé ainsi qu'à tout professionnel intervenant dans le système de santé. Toutes les personnes en contact avec le patient, qu'elles exercent ou non une activité médicale, sont tenues au secret médical. De la protection de la vie privée, source principale du secret professionnel, découlent, d'une part, le droit à secret des informations personnelles lors du traitement automatisé des données à caractère personnel[114] ou des échanges de données et, d'autre, part le droit à l'anonymat[115].

---

[107] Délibération de la CNIL du 4 février 1997 (*op. cit.*) et article R.710-5-12 du CSP.
[108] Article L. 365-2 du code de la santé publique et délibération de la CNIL du 4 février 1997.
[109] Article 45 du Code de déontologie médicale.
[110] Loi n°78-17 précitée et modifiée par la loi n° 2004-801 (*op. cit.*) ; Directive n°95-46 (o*p. cit.*)
[111] Dans ce cas, le consentement du patient n'est pas requis.
[112] Article L. 1112-1 du Code de la santé publique.
[113] Excepté dans les cas de dérogation expressément prévus par la loi, le secret couvre l'ensemble des informations concernant la personne prise en charge et portées à la connaissance du professionnel de santé, de tout membre du personnel des établissements ou organismes participant à la prévention et aux soins et de toute autre personne mis en relation, par ses activités, avec ces établissements ou organismes. Il s'impose ainsi à tout professionnel intervenant dans le système de santé.
[114] Article 226-16 du Code pénal.
[115] Protection des VIP, des malades atteints de pathologies soumises à déclaration obligatoire, traitements statistiques, etc.

Selon le Dr Michel DUCLOUX, président du CNOM, il faut « préserver à tout prix la confidentialité et l'intimité des gens. Sauf intérêt du malade, on ne doit pas pouvoir accéder à des dossiers sensibles tels que les données psychiatriques (…). Le secret médical, ce n'est pas pour protéger le médecin mais pour protéger le malade »[116]. Institué dans l'intérêt du patient, il « couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession…»[117] et s'impose à lui.

B) Textes techniques applicables en matière de sécurité du système d'information

Il s'agit essentiellement de normes, recommandations et études dont nous citerons ici seulement les principales.

Il n'existe pas de norme ISO spécifique traitant de la sécurité des systèmes d'informations de santé, mais seulement une norme générale : l'ISO 17799[118]. Cette norme d'origine britannique, élaborée par des grandes entreprises et adoptée par l'ISO en 2000, identifie 128 mesures de sécurité, de bonnes pratiques afin d'accompagner l'élaboration de la politique globale de sécurité de information.

L'ANAES a formulé des recommandations mentionnant la nécessité de sécuriser le système d'information et une nouvelle version intégrant les contraintes sécuritaires est à l'étude. De son côté, la CNIL a réalisé un guide des recommandations relatives au traitement des données de santé par les professionnels de santé. Dans une communication du 8 avril 2004, elle a émis un avis défavorable sur la création de bases de données d'empreintes digitales ou oculaires sur les lieux de travail en l'absence « d'impératifs de sécurité incontestables ». Interrogée sur cette notion, Jeanne BOSSI l'a rapprochée des principes de finalité et de proportionnalité : « des techniques de biométrie dans des fichiers informatiques doivent être justifiées par la finalité poursuivie : ainsi une cantine scolaire pourra instituer un contrôle palmaire pour contrôler le passage des élèves à la cantine mais non pas un contrôle de l'iris ».

Enfin, nous nous sommes intéressée aux études du Groupement de Modernisation du Système d'Information Hospitalier sur la politique de sécurité cadre. Le GMSIH fournit en effet un référentiel de bonnes pratiques, des outils méthodologiques ainsi que des recommandations techniques aux établissements de santé afin qu'ils puissent élaborer leur plan d'action en matière de protection de données de santé à caractère personnel. C'est l'objet du livrable sur la « Sécurité des Systèmes d'Information

---

[116] Propos extraits de l'article « Le Dr Michel DUCLOUX : une extrême vigilance s'impose », *Le Quotidien du médecin*, n° 7568, p. 3.

[117] « …c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris », Décret du 6 septembre 1995 portant Code de déontologie médicale, article 4.

[118] Norme d'origine britannique, élaborée par des grandes entreprises et adoptée par l'ISO en 2000, qui identifie 128 mesures de sécurité, de bonnes pratiques afin d'accompagner l'élaboration de la politique globale de sécurité de information.

dans les établissements de santé»[119]. Cette politique de sécurité cadre sert de base à la définition, par les établissements, de leur propre politique de sécurité, adaptée à leur niveau, à leur organisation et à leurs moyens.

2 VISIONS ET DIVISION DES ACTEURS

2.1 La sécurité informatique au cœur des « champs de force » : Un jeu de pilotage décisionnel et stratégique à flux tendus

La partie informatisée du SIH a pendant longtemps eu mauvaise presse au CH Montperrin. Coût élevé, partage dangereux de l'information et dysfonctionnements sont autant d'arguments qui ont ralenti l'évolution du SI. Si l'établissement accuse un retard dans ce domaine, c'est essentiellement en raison des préoccupations des différents acteurs en matière de sécurité de l'information qui sont venues en circonscrire l'évolution et en restreindre le développement.

2.1.1 Premier acte : Consensus…

A) Genèse d'un projet ambitieux

Au sein du CH Montperrin, une réflexion commune de la Direction, de la DSIO, de la CME, du CIM et des représentants des soignants est initiée depuis quelques années déjà ; le bureau de la C.M.E., la direction et la DSIO travaillant au projet de réseau depuis 2002. Lors de la CME de mars 2003, le Directeur rappelait son souhait de travailler « dans un climat de confiance » dans ce domaine central qu'est la transmission des informations au sein de l'établissement. Tous les médecins ont reconnu lors de cette CME que « le dossier était difficile ».

Un comité de pilotage (COPIL) a été institué début 2003, représentant toutes les composantes de la communauté hospitalière. Ce COPIL est conçu comme une instance stratégique de la politique de mise en œuvre du système d'information dont le rôle est de définir les responsabilités et les rôles, les méthodes et les procédures, d'approuver et de

[119] Consultable sur le site du GMSIH : www.gmsih.fr Le GMSIH accompagne actuellement quatre sites pilotes dans l'élaboration de la politique de sécurité : le CH de Chambéry, le CHI de Fréjus Saint-Raphaël, le CHR d'Orléans et le CH de Sens. Si le CH Montperrin n'a pas pu bénéficier de l'accompagnement proposé, il est néanmoins adhérant du GMSIH et a pu disposer des livrables réalisés par le Groupement.

supporter les initiatives de promotion et de communication internes[120], avant approbation définitive devant les instances[121] et insertion dans le projet d'établissement. Une large implication du corps médical dans la sélection et l'implémentation était indispensable, car un système d'information à visée médico-administrative est voué à l'échec sans le soutien des médecins. La stratégie choisie et en même temps inévitable à Montperrin fut donc de s'assurer l'assistance des médecins leaders, tout en arguant l'objectif de bien collectif. Pour des raisons pratiques et pour leur conserver un aspect opérationnel, deux groupes de travail ont été constitués à partir du COPIL selon une dimension fonctionnelle : un groupe médico-soignant et un groupe technico-administratif qui confronteront leurs travaux en séance plénière. Dès le début était donc officialisé le travail en commun. Le management de projet choisi au CH Montperrin est à la frontière entre le modèle bureaucratique et le modèle entreprenarial en combinant leurs vertus respectives : le management bureaucratique peut être un outil de coordination et de contrôle favorisant un ordre social stable ; parallèlement, le modèle entreprenarial, qui fait son entrée dans les organisations modernes, offre la flexibilité qui manque à l'autre modèle. On y retrouve la Direction, fonction décisionnelle qui définit la politique générale et contrôle les coûts d'opération, les utilisateurs – actuels et futurs – qui représentent la fonction de consultation et de réflexion et dont le rôle est d'exprimer leurs besoins et leurs contraintes en terme d'information et d'informatique, et enfin les informaticiens, fonction exécutive qui représente la partie experte. Les objectifs, la méthode, les comportements ne sont pas décidés par le seul sommet hiérarchique, mais sur la base de la délégation, de la confiance, et de la flexibilité. Ce type hybride de management se veut un outil de gouvernance qui n'altère pas la centralisation du pouvoir mais met en place des mécanismes d'autorité plus doux tout en conservant une surveillance continue. Cette combinaison[122] est délicate à réaliser, la politique poursuivie n'étant plus élaborée par le sommet mais soumise à la transaction dans sa phase d'élaboration et la DSIO étant chargée de conserver cet équilibre fragile. Face à cette dernière, on trouve essentiellement un triumvirat médical, leaders de la politique médicale de l'établissement et qui occupent les fonctions clé depuis 10 ans : la présidente de la CME, la présidente du Collège de l'information médical, le Président de la SMTEIM.

Un travail de fond a été initié entre mars et juillet, la réflexion sur le contenu du dossier médical étant repoussée, en l'absence de dossier informatisé. Comment ce travail pouvait-il dès lors être initié sur de bonnes bases, alors qu'une réflexion sur la politique de sécurité informatique doit au moins être concomitante de celle sur le DMP ?

---

[120] Politique de sécurité, charte utilisateur, SDSI en particulier.
[121] Collège de l'Information Médical, Conseil d'Administration, Commission Médicale d'Etablissement, Comité Technique d'Etablissement.
[122] Des modèles bureaucratique et entreprenarial.

B) L'appel à un cabinet de conseil

L'importance des enjeux de l'informatisation et la complexité de la problématique de la sécurité dans ce domaine rendaient nécessaire la réalisation d'un audit et la rédaction d'une politique de sécurité. La DSIO et le Comité de pilotage ont pris l'initiative de confier à un cabinet d'audit et de conseil spécialisé la mission d'assistance à la réalisation d'une politique de sécurité, à la formalisation du schéma directeur nécessaire à la poursuite des opérations d'informatisation de l'établissement et à la rédaction d'une charte utilisateurs. L'objectif de cette entreprise était d'étudier les failles de sécurité du réseau, point d'achoppement et cause de « gel du dossier », de l'aveu de la présidente du CIM à la CME de juillet 2003. La méthodologie mise en œuvre pour concevoir la politique de sécurité retenait comme principe premier la spécificité de la construction et son adaptation à la réalité du CH Montperrin. Cela supposait dès lors la participation active des acteurs[123] à la définition de cette réalité et au choix des principes, procédures, moyens et organisation ainsi que leur acceptation d'un échange entre les représentants des différents corps et leur confiance dans la méthodologie employée pour accélérer la réflexion sur le fond.

Les membres du cabinet d'audit nous ont confirmé que les objectifs du projet avaient été ciblés par les membres du COPIL. La nécessité de la conciliation avec des normes et référentiels externes a également été soulignée et rappelée par le cabinet à des multiples reprises, « la spécificité reconnue de l'établissement ne devant pas conduire « à une marginalisation par rapport aux réalités actuelles et à venir du secteur santé social », comme le rappelle l'une des personnes du cabinet interrogée sur la question.

A côté de ce COPIL, un groupe opérationnel composé de la DSIO, d'informaticiens et de nous-même, a été chargé de traduire les considérations stratégiques générales en caractéristiques fonctionnelles et de mettre en place cette nouvelle architecture, avec l'aide de la société de conseil.

Il s'agit là du premier acte d'un long spectacle qui frise parfois, comme nous allons le voir, le « vaudeville »[124].

2.1.2 Deuxième acte … « Dissensus » …

A) Un quiproquo déterminant

[123] L'implication de l'utilisateur dans la conception et la gestion du SIH est prévue dans le chapitre du manuel d'accréditation de l'ANAES.
[124] « Comédie légère dont l'intrigue repose sur des quiproquos », Dictionnaire de la langue française, Hachette, 1998.

Le corps médical s'est très vite arc-bouté sur les notions de droits d'accès, de partage d'information et de confidentialité. Comment ce projet pouvait-il évoluer favorablement s'il n'était pas jugé utile et bénéfique par les professionnels de santé ? Le choix de participer, de s'associer à un processus, d'être le cas échéant un élément moteur dépend en effet essentiellement des aspirations personnelles des acteurs.

Le recueil et l'analyse des besoins des utilisateurs sont une étape forte de la conception d'un SI sécurisé. La tâche se révéla d'une grande complexité dans l'établissement. Les besoins des utilisateurs doivent être satisfaits, mais encore faut-il pouvoir les identifier clairement, ce qui implique une démarche participative et volontariste de ces derniers. Pour établir une politique de sécurité, il convient préalablement de définir les besoins de partage en classifiant les informations et en les regroupant dans des catégories homogènes. Puis il est souhaitable *a minima* de conférer une note, un label, un indice de besoin (de 1 à 4) pour chaque parcelle d'information, en fonction de chaque catégorie d'utilisateurs concernée (secrétaire médicale, cadre de santé, médecin, médecin chef, bureau des entrées etc.). Idéalement, il conviendrait même de donner une note à chacune des propriétés de la sécurité : confidentialité, intégrité, disponibilité, auditabilité. Or, non seulement ces deux dernières étapes n'ont pas pu être franchies, mais la première, celle de la classification, a demandé de nombreuses réunions des sous-groupes du COPIL et de ce dernier pour finaliser une grille incomplète - et déconnectée de la réalité- d'expression des besoins de partage qui a finalement été mise de côté, les membres du COPIL ne parvenant pas à un consensus. Les médecins interrogés nous confient qu'une grille inadéquate leur a été imposée puisque les items repérés n'étaient pas ceux qui étaient utilisés dans la pratique et que les besoins en extra-hospitalier n'étaient pas recensés, « alors que les trois-quarts de patients sont vus en extra-hospitalier » précise la présidente de la CME.

Malgré les efforts déployés par ces derniers, une confusion est très vite apparue entre expression des besoins de partage et revendication des droits d'accès, devenue très vite source de blocage après quelques semaines de travail sur la question. La présidente de la CME, qui est également membre du CIM et vice-présidente de la conférence des présidents de CME de CHS, attribue ce blocage à une incompréhension mutuelle et au fait « qu'à Montperrin plus qu'ailleurs, les médecins s'occupent beaucoup plus d'information médicale »[125]. Questionnée sur ce blocage, la présidente du CIM reconnaît qu'un « malentendu, un symptôme d'incommunicabilité partagée » a été à l'origine du « gel du dossier » et précise que la DSIO se référait au partage d'information en général alors que les médecins envisageaient le partage d'information informatisée et campaient sur le préalable de la définition des droits d'accès en amont de toute

[125] Entretien en date du 10 septembre 2004.

formalisation du tableau d'expression des besoins de partage. Là était donc le nœud du quiproquo, qui ne pouvait être dénoué que par les médecins. Le chef d'établissement explique cette incommunicabilité par une « incompréhension persistante » mutuelle dans le domaine de la gestion des droits d'accès aux documents enregistrés dans les ordinateurs des services de soins et dans le domaine de l'élaboration du dossier médical informatisé. Le DIM, qui fait partie du CIM en tant que « technicien », mais dont l'aura l'a placé au sommet des leaders médicaux, n'a quant à lui pas souhaité répondre à nos questions sur cette «incommunicabilité ». Dans ce contexte, le cabinet d'audit s'est orienté vers la rédaction d'u document intermédiaire, « compte tenu des attitudes, comportements et difficultés aiguës rencontrées à l'occasion de la construction de la seule « table d'expressions de besoins de partage d'information »[126]. Cela était probablement préférable à une analyse des besoins validée mais erronée, bien que encore une fois, il reste difficile de concevoir une politique de sécurité qui ne soit pas fondée sur une définition claire des besoins de partage.

B) La crise du processus de décision

Le cabinet a été très vite perçu comme un « expert-complice » de l'administration, qui souhaitait, pour reprendre les termes de la présidente du CIM, « dupliquer un système adapté à l'entreprise, et non à la spécificité psychiatrique ». Les médecins interrogés avaient en effet le sentiment que le cabinet s'obstinait à ne pas aborder la question préalable de gestion de l'attribution des droits d'accès aux documents situés dans les ordinateurs de soins et que, par ailleurs, le traitement de cette question devait être concomitante à l'élaboration du dossier médical informatisé. La présidente de la CME, qui fait partie du CIM et du COPIL, précise « Nous ne sommes pas Nestlé ou Danone (…) les médecins se sont sentis considérés par la société de conseil comme du sous-personnel ». Enfin, d'après les termes de la présidente du CIM, ils appréhendaient un « choix sur-contraint » par les orientations formulée par le cabinet d'audit. Or, cela révélait d'une part leur sentiment de « dépassement » dans ce projet et, d'autre part, leur méfiance, alimentée par leur manque d'expertise dans ce domaine technique, vis-à-vis du discours « technocratique » de la société d'audit. Du reste, il leur avait bien été précisé que l'architecture en réseau projetée intégrerait la gestion des informations médicales et le dossier de soins. En réalité, l'une des inquiétudes majeures du CIM portait sur « le rôle spécifique et la responsabilité du CIM, notamment quant à la détermination des droits d'accès et des règles de traçabilité », constate le Directeur. Il leur a été clairement répondu, par courrier, qu'une des raisons du choix du Cabinet X était justement « son

[126] Entretien en date du 4 mai 2004.

indépendance par rapport à tous les fournisseurs de solutions logicielles ou matérielles », cette indépendance étant garantie par le statut même de la société et sa déontologie. Il a clairement été précisé par la Direction que « le choix du logiciel du dossier médical du patient relève de la compétence du CIM et de lui seul » ; les seules contraintes qu'il devra cependant respecter étant celles énoncées collectivement par la politique de sécurité et à travers les règles d'intégration et d'interfaçage édictées par les normes et recommandations ministérielles. S'engageant officiellement, en septembre 2003, à se consacrer à la phase de concrétisation, la direction n'a pas hésité à rappeler que « tout établissement hospitalier est un ensemble cohérent, multipartenarial au sein duquel le patient et la gestion de son dossier sont des éléments majeurs ». L'essai sera plus difficilement transformable qu'au CH E. Toulouse, établissement spécialisé en psychiatrie situé dans les bouches du Rhône et où la levée des boucliers n'émane pas des médecins mais des soignants : « nous souhaitons nous orienter d'ici deux ans vers un dossier médical informatisé mais nous sommes conscients que le risque de refus des utilisateurs en matière de dossier de soins unique informatisé viendra davantage des soignants (…) ; le corps médical est relativement passif » nous indique son DIM[127], sans que ce refus soit insurmontable puisqu'il ajoute « cette résistance porte sur le matériel, l'ergonomie, et non sur le partage des données ».

2.1.3 Troisième acte : …modus vivendi

A) Une nouvelle orientation stratégique

Pressentant les difficultés d'adhésion de l'ensemble des acteurs impactés, compte tenu de l'expérience de l'établissement en la matière, et agissant à la fois comme figure de proue et comme leader tentant de motiver les acteurs, la DSIO est passée par une période d'interrogation sur le bien fondé, la nature de son rôle et le sens de son action. A ce stade, le soutien de quelques médecins et paramédicaux s'est révélé très important mais insuffisant pour débloquer la situation. La prise de risque a pu paraître parfois trop importante. Devant les réticences opposées par le corps médical, à peine voilées derrière un attentisme de blocage, l'établissement a connu un moment d'essoufflement des acteurs et un désinvestissement passager du cabinet d'audit. Devant ce cas complexe, où il devenait impossible de poursuivre le travail au sein du COPIL, et après une tentative de médiation infructueuse entre les membres du corps médical et les auditeurs, la DSIO a choisi de rompre officieusement les modes opératoires protocolaires devenus inadéquats au regard de la réalité du travail. Elle a décidé de poursuivre la mise en place de la

[127] Entretien en date du 5 mai 2004.

politique de sécurité au sein d'un petit groupe opérationnel dépourvue de représentants médico-soignants. Ce groupe, coordonné et encadré par nos soins, dans le cadre du stage professionnel, et composé d'interlocuteurs de la société d'audit, de l'équipe informatique et de la DSIO s'est vu assigner la tâche de proposer en dernier ressort des documents finalisés, des plans d'actions correctives au COPIL, afin que ce dernier formule ses observations et valide, le cas échéant.

Après quelques mois, gardant à l'esprit les conséquences des solutions proposées sur l'ensemble de l'organisation et ne perdant pas de vue le conflit qui venait de se jouer, la DSIO a souhaité s'assurer que les membres du COPIL soient de nouveaux associés au processus sinon de conception, qui était largement abouti, du moins décisionnel quant à la forme finale de la politique de sécurité. Usant d'outils d'intégration externes depuis le début du processus[128], la Direction et la DSIO souhaitaient obtenir une validation formelle, étant entendu que le COPIL devait examiner et approuver formellement les spécifications retenues. En septembre 2004, la réunion du COPIL se conclut par l'entérinement d'avancées significatives : validation du plan d'actions, d'une politique de sécurité intermédiaire et de procédures types.

B) L'ère du soupçon n'est pas révolue

Plus d'un an après son institution, force est de constater qu'après des phases de solidarité, de coopération, de concurrence, de division et de blocage, un consensus global commence à émerger au sein du groupe.

Aujourd'hui, les membres du COPIL reconnaissent le malentendu et tentent de retravailler les énoncés des besoins en information c'est-à-dire de déterminer les personnes qui ont besoin des informations et le type d'information concerné, l'attribution des droits d'accès venant après. L'attitude d'un certain nombre de médecins a changé, y compris celle du « triumvirat » médical.

Si la présidente du CIM reconnaît que, quatre ans auparavant, « pour s'entourer des meilleures garanties, le corps médical ralentissait le processus de décision relatif au projet de réseau informatique », aujourd'hui en revanche les médecins ont pris conscience de son aspect incontournable et d'un probable « accouchement dans la douleur ». Elle reconnaît qu'elle-même n'accorde qu'une confiance relative à l'actuel système d'information reposant sur le papier et l'oralité. C'est d'ailleurs pour cette raison que les fax échangés dans l'établissement sur l'état d'un patient sont anonymés et accompagnés d'un appel téléphonique de nature à préciser l'identité du patient. Cette technique n'en reste pas moins, pour reprendre ses termes, « de l'artisanat ». L'ensemble

[128] Distribution systématique de comptes-rendus, rapports d'avancements transmis par la DSIO au COPIL, etc.

des professionnels de santé considère qu'un système d'information informatisé favorisera la qualité de l'information et le respect des règles déontologiques, 75% d'entre eux considèrent cependant qu'il devra être davantage sécurisé que le dossier papier[129]. La constitution de fichiers nominatifs contenant par nature des données sensibles en psychiatrie représente également selon eux un danger collectif, et appelle une vigilance permanente. L'un des dangers du développement de l'informatique hospitalière identifié par les médecins est la possibilité offerte de violer le système d'information pour déterminer les comportements des médecins eu regard de telle pathologie, crainte que partage E. DUSEHU[130].

Le travail de sécurisation du SIM est donc essentiel, notamment pour restaurer les confiances des utilisateurs. En effet, ils sont 46% à ne pas partager les informations par voie informatique en toute confiance alors que 79% des utilisateurs du SIA se disent confiants.

2.2 Les freins à la mise en place d'une politique de sécurité informatique

Si le CH Montperrin connaît depuis peu une période de transition favorable à la poursuite du déploiement du SI, il a rencontré et continuera probablement à rencontrer, bien que de manière plus ténue, en particulier sur la question sécuritaire, de nombreux obstacles techniques, méthodologiques, organisationnels et culturels.

2.2.1 Les causes conjoncturelles

A) Propres au CH Montperrin

a) Le secret médical et la confidentialité : syndromes ou garde-fous ?

La confidentialité est généralement associée au secret professionnel[131], et plus particulièrement, à l'hôpital, au secret médical[132]. Le secret médical, cette « chose

[129] *Cf*. annexe I.
[130] Qui nous enseigne que les industries pharmaceutiques payent jusqu'à 20 euros une ordonnance de médecin photocopiée et anonymée !
[131] Tel qu'il est institué dans le code pénal pour toutes les catégories de personnel : article 226-13.
[132] *Cf*. Décret n° 95-1000 du 6 septembre 1995 portant Code de déontologie médicale et l'article L 1110-4 du Code de la Santé Publique, instauré par la loi du 4 mars 2002.

sacrée » dont parlait Hippocrate[133], constitue l'obstacle premier à la transmission informatisée du dossier médical. Derrière la persistante résistance médicale à partager l'information concernant les patients, nous avons perçu au fil de nos entretiens, la peur de la levée du secret, la peur de l'intrusion, voire celle, non avouée, du jugement des pratiques médicales. « L'informatique a été et reste encore aujourd'hui une des grandes peurs du monde hospitalier (…) Parmi les causes de ce rejet, la crainte du personnel médical et soignant en matière de secret professionnel figurait en bonne place », note F. PONCHON, dans son ouvrage *Le secret professionnel à l'Hôpital et l'information du malade*[134]. Le secret devient alors un outil de rétention d'information et donc aussi un facteur d'abus de pouvoir, puisque la maîtrise de l'information est un enjeu de pouvoir. C'est précisément cet enjeu de pouvoir qui explique, selon le Directeur des soins, « le blocage du corps médical ».

« Le secret médical ne doit pas être l'épouvantail qui empêche l'informatisation : on peut entrer dans un service de soins en blouse blanche et voler aisément un dossier papier » affirme sans ambages E. DUSEHU, tout en reconnaissant que le secret médical protège davantage le médecin que le patient. G. MOSNIER le rejoint sur cette idée « le secret médical protège surtout l'équipe et accessoirement le patient ». En psychiatrie, cette dernière assertion nous semble devoir être nuancée : les patients doivent être particulièrement protégés car les informations qui le concernent peuvent être stigmatisantes, qu'ils fassent l'objet d'une mesure de protection judiciaire (sauvegarde de justice, curatelle, tutelle) ou qu'ils soient hospitalisés sous contrainte[135] (HDT, HO), et enfin en raison de la nature de leur pathologie (schizophrénie, psychose, etc.).

Le partage des données de santé confidentielles ne pouvant être réalisée que dans l'intérêt du malade[136] et sous la responsabilité du chef de service, pour assurer la cohérence des soins, le secret médical doit pouvoir être partagé. Le passage du secret médical stricto sensu au secret partagé, étendu par la Loi Kouchner du 4 mars 2002 aux équipes[137], est théoriquement bien implanté dans les consciences des médecins et justifierait l'abandon du terme d'information médicale au profit d'information de santé, laquelle englobe l'ensemble des données personnelles utilisables par les acteurs participant au processus de santé d'un patient. En organisant, par dérogation, un secret partagé, la loi poursuit comme objectif d'assurer la continuité des soins et de prendre en compte les évolutions de la prise en charge et la nécessité de conforter les réseaux de

---

[133] « Les choses que je verrai ou que j'entendrai dire dans l'exercice de mon art, ou lors de mes fonctions dans le commerce des hommes, et qui ne devront pas être divulguées, je les tairai, les regardant comme des secret inviolables » (Serment d'Hippocrate, V^{ème} S. av. J.-C).

[134] Berger-Levrault, Paris, 1998, p. 105.

[135] L'hospitalisation sous contrainte est strictement encadrée par le CSP : articles L3211-1 à L. 3215-4.

[136] Article 11 du Code de déontologie médicale : le secret médical ne peut être opposé que dans l'intérêt du patient ; article 12 : le médecin est responsable de la surveillance du comportement de ses assistants par rapport à ce secret ; article 13 : le médecin est responsable des accès illicites à son fichier clinique.

[137] Repris par l'article 2 de la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie.

soins qui multiplient les échanges d'informations. La grande majorité des médecins et des soignants interrogés constate que le secret partagé ne rencontre plus d'obstacle aujourd'hui. Pourtant, G. MOSNIER, interrogé sur la notion de dossier partagé, reconnaît qu'elle pose encore aujourd'hui des questions éthiques, « car le fait de partager le dossier n'est pas dans la culture hospitalière (…) le secret partagé n'est parfois qu'un mot et la rétention des informations par le corps médical reste d'actualité ». Pourtant encore, l'exemple de la mise en place de la décentralisation des plannings dans les unités de soins révèle une autre réalité ? Nous avons pu constater, alors que nous étions chargée de recenser les plannings de l'ensemble des personnels non médicaux, la réticence pour ne pas dire le refus des cadres de santé de s'immiscer dans les plannings autres que soignants dont la gestion dépend du médecin chef de service. Alors que les cadres avaient recensé les plannings des soignants, des aides-soignants et des agents de service hospitalier à la date requise, les médecins eux-mêmes ont dû être rappelés à l'ordre par plusieurs courriers officiels pour recenser ceux des assistantes sociales, secrétaires médicales, psychologues, etc. De même, lorsqu'il fut question de recenser les besoins de partage d'information, les médecins ont développé une telle vision maximaliste de la notion de donnée nominative qu'elle aurait presque été de nature à entraver le travail des secrétariats médicaux et du bureau des entrées, par exemple. Nous nous rappelons alors qu'à la question « Les personnels médicaux confient-ils facilement les informations médicales nominatives à l'équipe soignante concernée ? », E. DUSEHU avait répondu catégoriquement « non ! ». La présidente de la CME, quant à elle, avoue faire « parfois de la rétention d'information en réunion d'équipe, dans l'intérêt du patient, car l'être humain est faillible ». Après précision, nous comprenons que c'est l'infirmier qui figure ici l'être humain.

« Le respect de la confidentialité ne sera pas pire que ce qui existe actuellement » confiait en 1997 le président du CNOM, le Professeur Bernard GLORION, mais « il faut être vigilant et connaître les destinataires des informations transmises ». Selon l'un des membres du CIM, « la priorité des psychiatres est de préserver l'intimité de que disent les patients qui se déshabillent ».

Le principe du secret médical est propice à la confusion entre sécurité et confidentialité. Les nombreuses faiblesses énoncées par le rapport d'audit, alors même qu'elles étaient essentiellement centrées sur le SIM, ont apporté de l'eau « au moulin de la confidentialité ». La présidente du CIM souligne que « des patients renoncent à se faire soigner en psychiatrie si le secret médical et la confidentialité ne sont pas assurés de façon irréductible »[138]. C'est cet aspect qui reste « très difficile à faire passer aux administratifs, et surtout aux techniciens, même si ces derniers disent être soumis au

[138] Entretien en date du 06 septembre 2004.

secret professionnel » et qui commande parallèlement l'attitude du CIM et ses exigences de garantie et de plus grande maîtrise. Les techniciens (informatiques) ont, selon elle, une « fausse conception du secret » et en particulier du secret partagé. En effet, ils ne voient pas d'obstacle à ce que tout médecin puisse accéder au dossier d'un patient, en raison même de son appartenance au corps médical et de sa soumission au secret médical, alors qu'en psychiatrie plus qu'ailleurs il ne suffit pas d'être médecin pour pouvoir connaître la situation d'un patient ; encore faut-il faire partie des professionnels qui le soignent directement. Le secret médical est très réglementé et limité à la nécessité de dispenser des soins. Certes, le secret est partagé mais il doit être admis que chacun ne peut pas avoir accès à toute l'information. Il doit exister une hiérarchisation, des limites strictes et des accès définis à l'informatisation. A ce titre, la présidente du CIM, se remémore une expérience antérieure de réseau entre deux secteurs interrompue brutalement lorsqu'un médecin d'un secteur accéda à l'ensemble des données des patients de l'autre secteur. Pourtant nous dit-elle, les informaticiens n'y voyaient nul problème, « puisqu'il s'agissait d'un médecin ». Abondant dans le même sens, l'un des membres du CIM, qui est également vice-présidente de la conférence des présidents de CME de CHS et membre du COPIL sur le PMSI psychiatrique[139], insiste sur l'importance de l'étanchéité entre services et sur la nécessaire communication avec les structures ambulatoires dont dépend le patient soigné par le service.

b) Une sensibilité particulière de la notion « d'information médicale » en psychiatrie

La sensibilité des informations médicales a toujours interdit jusqu'ici leur traitement sur un système connecté au réseau. «LA CNIL reconnaît la spécificité des données psychiatriques comme plus sensibles, mais ne l'a jamais exprimé formellement », souligne Jeanne BOSSI, Chef de Division des Affaires publiques et sociales à la CNIL. L'ancien Président de l'Ordre National des Médecins, le Professeur Bernard GLORION, soutenait, le 1er octobre 1997, que l'informatisation « amène un changement radical mais elle ne va pas perturber la relation médecin-malade ». Etienne DUSEHU, interrogé sur cette même question abonde dans son sens[140].

Le RSSI des hôpitaux universitaires de Strasbourg constate que l'attitude du corps médical est partagée : une partie très « confidentialiste » tend à réduire la question de la sécurité à la notion de confidentialité, une autre n'y voit qu'un discours technologique et technocratique tandis qu'une dernière frange essaie d'en contourner les règles. Comme lui, la majorité des personnes interrogées au sein de la DSIO reconnaît qu'il est globalement plus difficile de discuter de la sécurité avec les médecins.

[139] Entretien en date du 10 septembre 2004.
[140] Entretien en date du 9 août 2004.

La diversité et le caractère particulièrement sensible des informations gérées par les établissements publics de santé impliquent une adaptation à chaque nature d'information.

L'ensemble des personnes interrogées au sein de Montperrin se représente la constitution de fichiers nominatifs contenant, par nature, des données sensibles en psychiatrie comme danger collectif. « Avec une simple prescription, on connaît la pathologie, or nous recevons des personnes en hospitalisation d'office ou encore séropositives », constate par exemple l'un des médecins, membre du CIM.

Un des cadres interrogés regrette que «tout soit de l'information médicale ou considéré comme tel (…) les médecins ne veulent pas que les soignants aient accès à leurs données, qui sont leur chasse gardée ».

c) Une conception large de l'information médicale qui englobe l'informatique

Cette confusion de la part du corps médical, et en particulier du DIM et du président du CIM, a été soulignée à plusieurs reprises par le DSIO et d'autres personnes interrogées sur la question ,au sein de l'administration.

La création des DIM dans les établissements de santé, se confondant initialement avec l'émergence des moyens nécessaires pour traiter localement de grandes quantités d'information, le recueil épidémiologique à partir de la fiche patient, outil de recueil épidémiologique, a été détourné de son objectif initial (décrire les présences de patients) pour être utilisé comme descriptif d'activité. Il n'est pas, dès lors, surprenant de voir se confondre information médicale[141] et informatique médicale. Parmi les disciplines médicales, la psychiatrie illustre le mieux cette conception étendue de l'information médicale. La frontière entre information nominative strictement médicale, informations partagées (médico-administratives) et informations non-médicales est plus tenue, mouvante, en raison de l'évolution des connaissances médicales et des conditions économiques, sociales et culturelles propres à la psychiatrie. C'est la raison pour laquelle il apparaît plus judicieux d'intégrer le traitement de l'information médicale dans le cadre juridique plus large de la donnée « nominative ».

Cette confusion entre information médicale et informatique explique en partie les difficultés rencontrées par le DSIO pour déployer des projets informatiques.

d) La crainte de la traçabilité ?

Le maintien de la règle ancienne est plus rassurant que sa transformation. Dans les années 80, le projet proposé par le FBI de développer un système informatisé national

[141] Selon L. DUSSERRE, l'information médicale est « l'ensemble des données destinées aux actions de nature diagnostique, thérapeutique ou de prévention », cette définition limite l'étendue aux données utilisées par les seuls professionnels de santé.

portant sur les dossiers criminels a été combattu par les Etats fédérés jusqu'à son abolition, à peine cette liste nationale constituée à l'échelle des Etats-Unis. Au même titre que les Etats ne souhaitaient pas que le gouvernement fédéral puisse surveiller l'usage qu'ils font des dossiers criminels, nos médecins psychiatres semblent, pour certains d'entre eux, embarrassés par la possibilité d'instaurer une traçabilité de leur pratique médicale. D'une part, les psychiatres nous semblent frileux lorsqu'il est question d'évaluation par les pairs. Nous entrevoyons derrière cette réticence un rejet de toute confrontation d'idée sur un même cas d'étude, voire, éventuellement, un manque de confiance vis-à-vis du confrère. C'est, du reste, peut-être aussi en partie pour cette raison qu'ils ont accueilli sans débordement d'enthousiasme l'accès direct au dossier médical. Imaginez leur circonspection pour ne pas dire leur suspicion devant le projet de DMP, annoncé par le Ministre de la santé P. Douste Blazy, et repris par la loi du 13 août 2004 relative à l'assurance maladie.[142] Ce projet de DMP a d'ailleurs été qualifié de « délirant » par E. DUSEHU, selon lequel il se résume à « un affichage politique ». Quoi qu'il en soit, c'est au projet médical de se prononcer sur l'orientation d'un dossier médical informatisé, et il revient au schéma directeur d'en fixer les contours. Or, le respect de la vie privée lors de l'utilisation des NTIC, la protection des données et la détection d'anomalies imposent une journalisation des actions qui surviennent dans le SI.

La traçabilité renforce le principe selon lequel un SIH doit être centré sur le patient et mis en œuvre selon une approche par les processus – la sécurité pouvant être considérée comme un processus de support du processus de production de soins –. Force est de constater les difficultés et retards de réalisation dans ce domaine. L'objectif n'est pas d'instituer un mouchard mais d'exploiter les fichiers dans le seul but de détecter les pannes, les actions illicites et les dysfonctionnements, d'y remédier ou encore d'identifier l'auteur d'infractions à la charte de sécurité par exemple.

Néanmoins, sécuriser le SI, c'est assurer que l'établissement exploite des fichiers dans le seul but de détecter les pannes et remédier aux pannes, dysfonctionnements ou actions illicites et d'identifier le cas échéant l'auteur de l'infraction.

Selon E. DUSEHU, « la traçabilité n'est pas une menace, mais permet de surveiller si la personne qui consulte une information est habilitée et n'outrepasse pas ses droits (…) il ne faut pas avoir d'état d'âme sur les suites disciplinaires à mettre en oeuvre le cas échéant ».

B) Propres à toute organisation

a) La résistance au changement

[142] n° 2004-810, article 5 (cf. annexe II).

La culture organisationnelle peut faire obstacle aux changements en particulier techniques, lesquels sont une menace pour les *a priori* et postulats qui fondent la culture d'établissement. Comme toute organisation très structurée, l'hôpital se caractérise en effet par une division nette du travail, des règles et procédures explicites et une hiérarchie très marquée que l'on retrouve dans la composition du COPIL du système d'information[143]. Bien que partant d'une volonté, affirmée par ses membres, d'avancer rapidement et efficacement sur ce dossier, très vite les ordres du jour chargés et la focalisation sur des points de détail ont enrayé la machine.

Nous avons vu que la résistance au changement au sein du CH Montperrrin est passée par plusieurs phases : le blocage passif puis l'activisme pour entrer aujourd'hui dans une période de lâcher-prise puisque les relations entre l'administration et les professionnels de santé se sont renouées de manière constructive sur ce difficile dossier qu'est la politique de sécurité. Il a surtout été suscité par le corps médical, les personnels soignants étant restés en retrait, contrairement au CH Montfavet où « les médecins sont restés neutres contrairement aux soignants qui ont présenté des réticences au projet de politique de sécurité et d'informatisation des unités de soins par peur d'être happés par le travail administratif » précise son Directeur, G MOSNIER, qui est également secrétaire général de l'ADESM.

b) La partition en champs de forces

Le monde social se décompose en une multitude de champs, pour reprendre la terminologie de Bourdieu, qui comprennent des enjeux, des objets et des intérêts spécifiques. Parmi ces champs différenciés et autonomes possédant des habitus – ou sens du jeu –, des points de vue, enjeux, des objets et des intérêts spécifiques, nous en en entrevoyons trois : le monde médical, le monde administratif et le monde soignant. A l'intérieur de ces champs de force, des agents oeuvrent pour acquérir le monopole de l'autorité en tant qu'elle octroie le pouvoir. Ceux qui dominent ce champ sont ceux qui disposent d'attributs valorisés par le champ : diplômes, connaissances, capacité oratoire, origine sociale, présentation de soi. Les champs dans lesquels s'inscrivent les trois mondes identifiés ne sont pas des structures figées. Au contraire ils se caractérisent, comme c'est le cas au CH Montperrin par des rapports de force issus de luttes intestines qui sont le fruit des stratégies des acteurs. Les administratifs cherchent à « imposer » un

[143] 3 représentants du corps médical – le fameux triumvirat-, 3 représentants du Service de Soins Infirmier (dont le D.S.S.I.), le pharmacien chef de service, le Directeur du système d'information, un ingénieur informatique, le Directeur de la communication, le Directeur du pôle patients, un ingénieur infrastructures, l'analyste de gestion, chargé du montage de la filière administrative

modèle cybernétique[144], les médecins, à défendre l'exception psychiatrique, les soignants, à prendre leur place.

c) Une sensibilisation récente des chefs d'établissements

Sans toutefois freiner le processus, la Direction ne s'est pas appropriée immédiatement ce projet. Il faut remonter à la source et comprendre que cette appropriation touche la construction proprement dite du système d'information, dont la politique de sécurité n'est qu'un élément. « Les chefs d'établissements ne perçoivent pas toujours l'importance fonctionnelle et stratégique de tels chantiers », constatait P. PEYRET il y a quelques années[145]. G. MOSNIER reconnaît quant à lui que l'ADESM ne sait pas penchée, à sa connaissance, sur la question de sécurisation du système d'information. Ce constat semble demeurer d'actualité, du moins au sein de notre terrain d'observation. En effet, à première vue, il semble que l'efficacité d'une politique de sécurité dépende au moins autant dans la technicité des mesures physiques et logiques et de leur cohérence que d'un volontarisme fort de la Direction Générale et de la CME sur le partage d'information, la DSIO étant plus spécifiquement chargée de faire des propositions en matière de sécurité des données. L'entretien avec le chef d'établissement nous éclaire sur son mode de management : leadership participatif fondé sur la négociation, la maturation et l'appropriation qui lui semble plus efficace au long cours qu'un management directif, certes efficace à court terme mais source potentielle de conflit social. Montperrin n'a pas choisi le modèle du «village gaulois » prôné par un des informaticiens, consistant à isoler les irréductibles et équiper les autres. Le directeur chargé des Affaires générales précise à propos de ce type de management : « le non dit fait partie de la technique décisionnelle, il permet de laisser mûrir les choses, et parfois ça marche (…). Par exemple, le corps médical est aujourd'hui ouvert à l'idée d'une équipe de sécurité (générale) qui ne soit pas soignante, or il y a six ans, cette proposition de la part de la Direction aurait été traitée de fasciste ». Par ailleurs, et pour mieux appréhender la démarche de la Direction, il faut reconnaître que les avantages à court terme restent assez mal définissables lorsque l'on n'est pas utilisateur du SI. S'ajoute à cela l'incertitude des choix technologiques et l'importance des investissements nécessaires[146]. Les dépenses dans ce domaine, et plus particulièrement celles d'exploitation, sont

[144] La cybernétique se décrit comme une «science du contrôle et de la communication», convaincue que tout comportement (humain ou non humain) s'explique fonctionnellement par rapport à un but et résulte d'une interaction informationnelle avec son environnement. Ce modèle est utilisé pour la description et la compréhension, entre autres, du monde social : le réel pouvant être interprété en termes de communication et d'information. Il permet donc l'analyse globale de la société et de l'influence des techniques de communication sur celle-ci.

[145] Directeur d'hôpital et professeur de gestion hospitalière à l'Ecole Nationale de la Santé Publique, il opère ce constat dans la préface de l'ouvrage de PONCON G., *Le Management du système d'information hospitalier. La fin de la dictature technologique*, Editions ENSP, 2000, p. 5.

[146] Une enquête réalisée en 2001 par le GMSIH auprès de ses adhérents montre une mobilisation insuffisante autour du thème de la sécurité informatique, qu'il explique par « une appréhension incertaine des directions générales sur

importantes et ne cessent de croître. L'augmentation du nombre des postes de travail, des imprimantes et des licences est identifiable tandis que celle de la maintenance ou encore des consommables et les besoins de formation est assez malaisée à Montperrin. Les incidences financières sont donc aujourd'hui difficiles à cerner. Le marché informatique est tout aussi déterminant. L'ouverture de l'hôpital à d'autres systèmes d'informations implique un suivi, plus assidu qu'auparavant, de l'évolution des techniques et standards du marché. Si l'impératif de sécurité informatique n'était pas perçu comme évident par la direction générale, le chef d'établissement était conscient de ses responsabilités économiques (tenue de la comptabilité sur informatique par exemple), réglementaires (respect de la réglementation sur les données à caractère personnel contrôlée par la CNIL) et juridiques (responsabilité pénale en matière de traitement automatisé des données).

2.2.2 Causes structurelles

A) Causes spécifiques à l'hôpital psychiatrique

Dans un esprit d'analyse socio-psychologique, il est intéressant de comprendre les motifs de résistance des utilisateurs propres au secteur hospitalier spécialisé en psychiatrie en étudiant, d'une part, la manière dont l'opposition est structurée et comment certains acteurs[147] influent sur les personnes et les groupes et, d'autre part, la perception de la politique de sécurité et l'utilisation de l'information formelle.

a) Une conception forte du secret et de la confidentialité

Si, aux Etats Unis, on peut trouver sur internet les CV des médecins, les sanctions reçues, leurs honoraires, la France est loin d'avoir atteint ce niveau de maturité et son secteur hospitalier psychiatrique l'est encore plus. Si l'on ne trouve pas comme en hôpital MCO la fiche de bilan au pied du lit en psychiatrie, le dossier papier, éclaté entre les services et pavillons est «sans doute, d'une certaine manière, plus dangereux que le dossier informatique », comme le soulignait déjà Claude Evin[148] en 1998. Les médecins du CH Montperrin en ont à ce point conscience qu'ils appliquent souvent moins le principe de précaution, alors même que l'urgence vitale est marginale comme nous l'avons vu, qu'ils ne souffrent du « syndrome » de précaution.

---

l'importance de la sécurité des systèmes d'information et une faible culture de la pratique de la sécurité », cf. livrable n°1 Politique de Sécurité des Systèmes d'Information des Etablissements de Santé, 31 mars 2003, p. 5.

[147] L'acteur est évidemment celui qui agit mais également celui qui joue un rôle, se met en scène selon la conception d'Irving GOFFMAN.

[148] Lors du débat organisé par le CNOM autour de la question de «La place du secret entre transparence et éthique professionnelle », 1er octobre 1998.

La transgression quotidienne du secret, bien qu'avouée de manière très édulcorée par les professionnels de santé lors de nos entretiens, est inhérente à l'organisation hospitalière en raison de la multiplicité des acteurs. Elle est plus particulièrement envisageable à l'extrémité de la chaîne : les informations sont transmises au médecin, au pharmacien, à ses collaborateurs, aux services de sécurité sociale ou encore à ceux de la DDASS (transmission des certificats d'hospitalisation d'office par fax, transmission d'un certificat médical de constat de fugue d'un personne hospitalisée d'office) dont les agents administratifs ne sont eux pas tenus au respect du secret médical mais à celui du secret professionnel.

b) L'éclatement pavillonnaire

Le CH Montperrin est un établissement de type pavillonnaire, ouvert sur des prises en charge extra-hospitalières très développées. La division des asiles d'aliénés en plusieurs unités architecturales complètement indépendantes les unes des autres remonte en fait à l'origine même de l'institution de ce type d'établissement, à la suite du célèbre rapport adressé par le médecin Etienne Esquirol au ministre de l'Intérieur en 1818.

Dans le cas d'Aix en Provence, le plan pavillonnaire fut adopté de façon précoce : l'établissement, à l'origine privé, présente déjà une telle disposition en 1875.

Cette configuration architecturale n'est, par nature, pas un terreau fertile pour le développement d'un système d'information unique ni pour l'émergence d'un consensus. Le contexte pavillonnaire interfère sur le fonctionnement de l'hôpital : l'information circule moins aisément que dans une structure monobloc, l'association de l'organisation sectorielle à la structure pavillonnaire participe à cloisonner les pavillons entre eux. Par ailleurs cette organisation structurelle se double d'une prise en charge sectorisée qui participe du cloisonnement des unités : les patients qui réalisent plusieurs séjours à l'hôpital se retrouvent dans l'unité de soins qui est du ressort de son secteur géographique. Si cette organisation est favorable au suivi personnalisé du patient par une même équipe, suivi qui est évidemment essentiel compte tenu des pathologies concernées, elle centralise le dossier patient à un endroit donné. En revanche, elle favorise l'échange des informations en extrahospitalier avec les CMP, CATTP et hôpitaux de jour. De manière paradoxale donc, la sectorisation psychiatrique est à la fois un frein et un levier à l'échange informatisé car elle connaît des besoins importants de communication qu'un réseau, reliant toutes les structures qu'elles soient éloignées ou pas, pourra combler en respectant les impératifs de sécurité liés aux droits des usagers.

E DUSEHU attribue en partie le retard de la psychiatrie dans le domaine de la communication informatique à la nature de l'institution psychiatrique: « ce n'est pas parce

que l'on décrète la psychiatrie hors les murs, qu'elle l'est ; l'évolution culturelle sera lente car les personnels ont toujours vécu dans l'enfermement ».

c) L'absence d'urgence et de protocolisation

« En MCO, on ne peut pas différer une intervention médicale, alors qu'en psychiatrie, s'il y a un minimum à mettre en œuvre pour traiter la crise, en particulier en cas d'hospitalisation d'office, les soins sont souhaitables mais s'ils ne sont pas réalisés, le patient ne décède pas », reconnaît le médecin DIM. Les obstacles rencontrés par l'administration pour conduire le projet d'élaboration de la politique de sécurité sont également liés à la déconnexion de la psychiatrie du reste du champ hospitalier : comment décloisonner les services administratifs et médicaux pour faciliter une véritable interopérabilité lorsque l'on n'est pas contraint par la tarification à l'activité ?

En l'absence d'urgence vitale pour le patient, les règles de travail ne sont pas toutes protocolisées, les acteurs réinventent et contournent les règles officielles, lorsqu'elles existent. Dans ce contexte, l'innovation requiert un bouleversement des mentalités, des efforts en terme d'investissement personnel et génère autant d'incertitudes qui sont sources d'un sentiment d'insécurité pour le corps médical en particulier.

d) Des rapports de pouvoir redistribués au profit de l'encadrement médical et administratif : un pouvoir de gouvernance DIM-Administration ?

« Tout dans cet établissement révèle des enjeux de pouvoir entre l'administration et les médecins, c'est une tradition montperrinoise », reconnaît la Présidente de la CME. Tout aussi difficile est la conciliation des objectifs de l'autorité « charismatique », le corps médical, et de l'autorité « légale rationnelle », la Direction[149]. La présidente de la CME nous a avoué avec un demi-sourire qu' « à Montperrin, les médecins se mêlent de tout, alors que le paramédical n'a pas pris sa place, en particulier les cadres soignants ». On retrouve, comme dans tous les hôpitaux, à côté des médecins cantonnés dans leur activité médicale, ceux qui, dans un hyperprofessionalisme exacerbé, s'approprient la gestion de l'hôpital et ceux qui participent de manière constructive à cette dernière. De même, au sein de la Direction, la réflexion est de plus en plus médico-administrative comme le démontre par exemple l'élaboration en cours du projet d'établissement 2005-2009, dans lequel l'administration empiète également sur les prérogatives des personnels médicaux, de l'aveu de l'un des directeurs-adjoints.

[149] Nous nous permettons ici d'emprunter les termes weberiens d'autorité « charismatique » et d'autorité « légale rationnelle » pour représenter respectivement le corps médical et la Direction administrative, sans pour autant les opposer. Cette terminologie nous a été inspirée de l'article de F. STEUDLER, Le management hospitalier de demain, approche sociologique, *Revue Hospitalière de France*, mars-avril 2004, n°497, p. 47 « il s'agit d'une sorte d'opposition entre l'autorité légale-rationnelle du bureaucrate et l'autorité charismatique du professionnel-médecin ».

L'innovation est extrêmement difficile à mettre sans l'appui du corps médical, l'autorité d'un directeur sur un médecin étant limitée par l'autonomie institutionnelle de ce dernier qui échappe par les textes à la dépendance hiérarchique.

Par ailleurs, l'institution d'une gestion bicéphale de l'information DSIO/DIM peut créer de la confusion dans la détermination des compétences respectives, d'autant plus que les missions du DIM sont plus clairement définies par les textes[150] que celles du DSIO[151]. « L'administration a longtemps été considérée par le corps médical comme l'intendance qui devait suivre en raison d'une conception mandarinale des directeurs d'hôpitaux. On était là pour commander les crayons et les tenir. Heureusement, les choses changent, mais lentement », précise un directeur adjoint.

Jeanne BOSSI voit dans la nature même de l'organisation hospitalière « un terreau plus propice à la séparation entre professionnels de santé et administration qu'à construction d'une préoccupation commune de sécurité informatique ».

Par ailleurs, la distance hiérarchique entre les catégories de personnels, du sommet jusqu'à la base, qui peut être gommée à l'occasion d'une tâche collective centrée l'intérêt immédiat du patient, est source de cloisonnement et de disjonction quand l'objectif est technico-organisationnel. L'autorité hiérarchique administrative sur les soignants perturbe également la donne. Si l'informatisation des unités de soins dans un premier temps et la construction d'un SI centré sur le patient augmenteront comme nous le pensons la responsabilité des fonctions soignantes, le rapport très paternaliste du médecin-chef de service, « seigneur en son fief », avec les infirmiers devrait s'en trouver profondément modifié. De la à supposer que l'une des réticences du corps médical devant le projet de SI interconnecté ou de DMP, provient de la crainte d'une remise en cause de l'ordre établi par le spectre de l'autogestion des personnels et de la décentralisation de la prise de décision, il n'y a qu'un pas.

A la question « les médecins accepteront-ils, selon vous, le changement impliqué et associé », l'un des membres du cabinet d'audit reste perplexe. Il attribue leur résistance passée, mais encore latente, à une « peur d'un pouvoir qu'ils n'exercent qu'à titre provisoire faute de réelle informatisation digne de son nom de la partie médicale du SI ». « Certains médecins n'ont pas encore totalement abandonné l'idée du pouvoir médical » confiait en mai 2000, le Président du CNOM, le Professeur Bernard Glorion[152].

---

[150] *Cf.* Circulaire 24 juillet 1989, *op. cit.*
[151] *Cf*. Circulaire du 6 janvier 1989 (*op. cit.)* qui confirme le rôle joué par le DSIO auprès du Directeur.
[152] Interview du 25 mai 2000, pour le magazine de la médecine électronique Medcost http://www.medcost.fr/html/contributions_cb/cb_090600b.htm

B) Causes communes à toutes les organisations

a) *L'inertie*

Puisqu'un système d'information est de nature à modifier la structure, les méthodes de travail et la culture de l'hôpital, il suscite des résistances lors de chaque transformation importante, car il est difficile pour une organisation de se substituer totalement et immédiatement à une manière de fonctionner archaïque. L'inertie de l'organisation hospitalière, organisation de type bureaucratie[153] professionnelle[154], c'est-à-dire fondée sur la connaissance et dont les produits et services dépendent de l'expérience et du savoir-faire de professionnels, a ralenti jusqu'ici les changements occasionnés par la technologie de l'information et les systèmes d'information. A chaque étape d'approfondissement de la rationalisation, de nouvelles incertitudes apparaissent, qui viennent créer du changement et du mouvement. Les organisations bureaucratiques sont vivement critiquées depuis les années 60 pour leur incapacité à s'adapter à une évolution rapide et en raison du manque d'autonomie dont jouissent les individus.

b) *La symétrie de l'ignorance*

Chaque personne à sa conception du système, ne reconnaît pas aisément le point de vue divergeant de son alter ego et ne sait pas communiquer efficacement avec un individu n'appartenant pas au sérail de sa catégorie professionnelle. C'est ce dilemme, la symétrie de l'ignorance, que l'on retrouve au CH Montperrin.

L'administrateur réseau le reconnaît «On communique pas assez à l'hôpital qui reste cloisonné. Ca fait partie de notre travail au service informatique de communiquer, or on ne le fait pas assez et mal ».

Comme les directeurs d'hôpitaux installés depuis plus de vingt ans dans leurs fonctions, les médecins n'ont, d'une part, pas bénéficié pendant leur cursus de formation d'un enseignement sur le système d'information hospitalier.

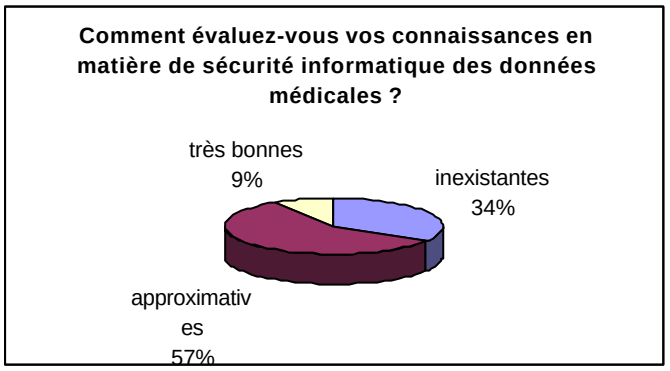
On note, d'autre part, un problème global de niveau de compréhension des questions informatiques de la part des soignants, admis comme tel par ces derniers, à l'exemple de ce cadre de santé avouant « je ne comprends pas grand chose, mais ça a l'air très bien », à propos du document exposant la politique de sécurité proposé à la validation en comité de pilotage le 21 juin 2004. On décèle le même problème chez le corps médical en général, de façon non avouée mais qui se déduit de sa focalisation sur des points de détail politiquement sensibles et sa déconcertante déconnexion sur les autres points. «On part d'assez bas dans l'établissement au niveau culturel » reconnaît

[153] Au sens où l'entend le sociologue allemand Max WEBER.
[154] *Cf*. la classification des structures organisationnelles de MINTZBERG.

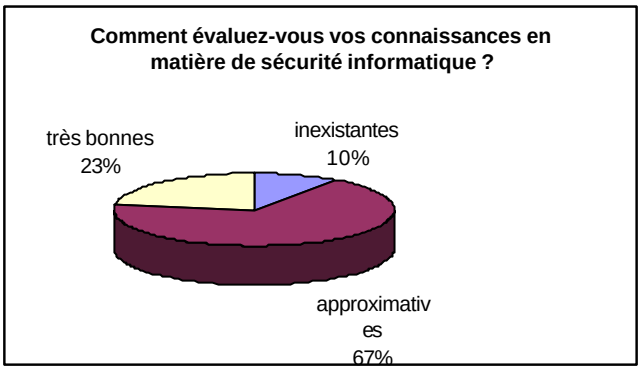
d'ailleurs la présidente du CIM ». Le niveau de complexité du projet est donc de nature à fragiliser l'équipe pluriprofessionnelle composant le COPIL, au sein de laquelle les significations et les enjeux de la sécurité diffèrent selon les positions occupées. Ce problème d'évolution culturelle dans le monde hospitalier, souligné par E. DUSEHU, qui attribue le retard en psychiatrie à «un manque de réalisme », avait été repéré par F. PONCHON : « Le médecin se sent dépossédé de ses informations quand il doit les partager, c'est culturel »[155].

Un tiers des professionnels de santé reconnaît n'avoir aucune connaissance en matière de sécurité informatique des informations médicales contre un utilisateur sur dix du SIA :

SIM



SIA



c) Des objectifs catégoriels à concilier avec l'intérêt général

L'élaboration d'un SI sécurisé n'est pas un processus totalement rationnel. Certains utilisateurs se servent parfois de leur pouvoir dans la structure, de leur respectabilité ou encore de leur aura pour poursuivre leurs intérêts personnels ou pour consolider leur position, plutôt que de porter et promouvoir les objectifs de l'organisation. Certains résistent même lorsqu'ils estiment qu'il nuit à leurs intérêts : la culture de l'individualité est très forte à l'hôpital. Nous verrons que bien que la majorité des médecins était plutôt favorable au projet de déploiement du système d'information et à sa sécurisation, le nombre importe peu en face de quelques fortes personnalités médicales charismatiques et jouissant d'un certain pouvoir dans le domaine informatique. Nous constaterons en effet que trois ténors sont suffisants pour freiner un projet, pourvu qu'ils occupent des fonctions clé dans l'organisation hospitalière. L'année 2003 a été marquée par « l'attitude réfractaire de certains intervenants » à l'uniformisation de l'ensemble des moyens informatiques à terme, comme le soulignait l'un des membres de la société d'audit[156]. Il nous confia même que cette attitude consistait « à ne pas coopérer franchement, à ne pas faire l'effort de travailler pour l'intérêt général de l'institution », ou

[155] PONCHON F., *op. cit.*, p.106.

encore « à ne pas hésiter à revenir sur les décisions prises en séance ». Le retard tient essentiellement aux résistances du corps médical dont la culture privilégie l'approche individuelle du malade sur la participation à un système de santé publique. Pour autant, il serait partiel de s'arrêter à cette version. Les stratégies d'usage développées par les acteurs sont donc éclairantes, bien que difficilement visibles et nécessitent un effort particulier d'observation, d'analyse et d'attention. Le Comité de pilotage, en tant que groupe de travail, se distingue de l'organisation tout en poursuivant les buts de cette dernière. Il constitue une catégorie *sui generis*, dotée d'une forme de sociabilité propre et de valeurs éthiques théoriquement partagées. Il est donc intéressant de prendre en compte les trajectoires, les identités et les aspirations des membres du groupe ainsi que les formes de solidarité et de contrôle qui s'exercent dans le groupe.

3 LA MISE EN OEUVRE D'UNE POLITIQUE DE SECURITE INFORMATIQUE INTERMEDIAIRE QUI POSTULE DE NOUVEAUX JEUX TECHNICO-ORGANISATIONNELS

Audit de sécurité, plan d'actions correctives, référentiel et charte utilisateurs, procédures types, schéma directeur, sont autant d'instruments qui participent de la constitution d'une véritable « politique de sécurité ». On peut distinguer plusieurs niveaux de mises en œuvre.

3.1 Un compromis entre besoins de partage d'information, vulnérabilité du système et contraintes normatives

Pour réduire les risques d'erreurs, de sinistres et les brèches de sécurité, il faut intégrer les méthodes, politiques et procédures organisationnelles particulières dans la conception et la mise en œuvre du SI sécurisé.

Le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la

[156] A l'occasion du travail de préparation de la réunion d'élaboration de la politique de sécurité du 6 mai 2004.

destruction accidentelle ou illicite, l'altération, la perte, la diffusion ou l'accès non autorisé. Ces mesures doivent assurer un niveau de sécurité adapté aux risques engendrés par le traitement et la nature des données à protéger, adaptés car les utilisateurs du SIM en particulier, s'ils considèrent les mesures de sécurité informatique justifiées, en revanche hésitent à se prononcer sur leur acceptabilité[157]. La conduite du projet doit prendre en compte la teneur du changement, qu'il soit organisationnel ou culturel et notamment les difficultés pour exprimer les besoins, la lourdeur et les délais de déploiement.

3.1.1 La politique de sécurité du système d'information : une orientation inéluctable qui s'insère dans une politique de gestion des risques

A) Une prise de conscience hospitalière des enjeux des menaces et des risques

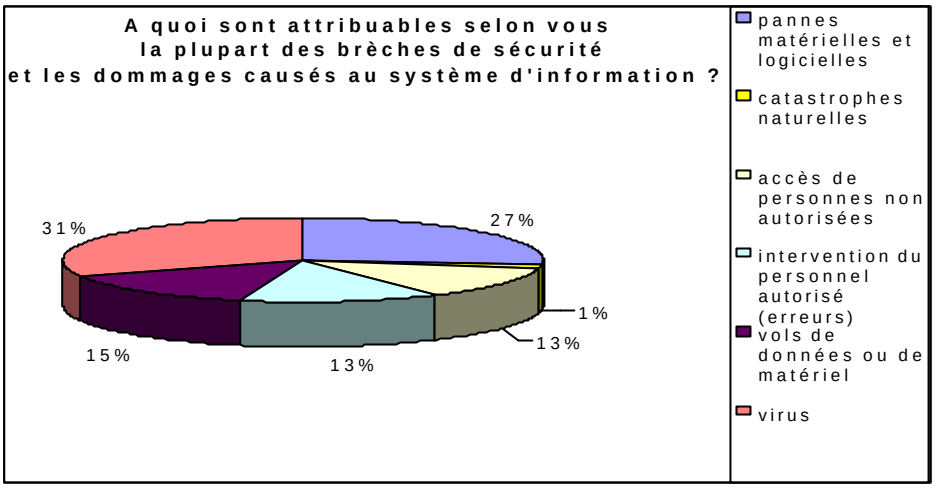
La libre circulation du dossier entre les services pose le problème de l'équilibre fragile entre le besoin du système qui, dans l'intérêt des patients, diffuse le maximum d'informations à un maximum d'utilisateurs habilités et les contraintes légales et le principe de la confidentialité auquel il se heurte.

Sinistres, virus, brèches de sécurité, logiciels et données défectueuses, usages abusifs, erreurs, fraudes menacent constamment tout système d'information.
Les risques encourus par un système d'information sont globalement de trois ordres : les accidents[158], les erreurs[159], les malveillances[160].

Si les pannes de matériel, les bogues de logiciel, les interruptions de communications, les erreurs humaines, les dégâts des eaux, ou encore l'usage par des personnes non autorisées peuvent entraver le bon fonctionnement d'un système d'information informatisé, la principale menace reste encore l'utilisateur habilité ! Le plus souvent, constate l'un des agents du service informatique, la plupart des altérations causées au système d'information, les brèches de sécurité, sont attribuables aux utilisateurs autorisés. La difficulté dans ce domaine est de « faire la part entre l'erreur, la négligence, le laxisme, la faute professionnelle et l'acte malveillant » comme l'indique L. Lamère[161]. Les utilisateurs du SIA énoncent, parmi les principales menaces, les virus, les pannes matérielles et les vols ; l'erreur n'est citée que par 13 % de ces derniers ce qui

[157] *Cf.* annexe I.
[158] Destruction partielle ou totale, dysfonctionnement des matériels, des logiciels et de l'environnement technique dont l'origine peut être un incendie, une panne électrique, un dégât des eaux, un choc, une exposition à une forte source de chaleur, etc.
[159] Lors de la saisie des informations, de leur transmission, de la manipulation (destruction des archives par exemple).
[160] Vol ou sabotage du matériel, copie ou destruction de fichiers de logiciels, intrusion de virus.
[161] LAMERE J.M., *Sécurité des systèmes d'information*, Paris, Dunod, 1991.

démontre qu'il reste encore à les sensibiliser sur leur part de responsabilité en matière de dommages causés au système d'information.



Aujourd'hui, il est possible de protéger les SI contre les invasions virales par des disquettes infectées provenant de sources extérieures, par des machines infectées ou par de fichiers ou logiciels téléchargés sur internet. Or, les liaisons à intranet et à Internet exigent l'adoption de mesures de sécurité particulières. La solution est simple : le pare feu et l'antivirus mis à jour quotidiennement.

Les systèmes d'information semi-automatisés qui fonctionnement imparfaitement ou sont mal exploités portent des germes de faille et de nuisance (risque de mauvais acheminement par fax, échange de données par disquette. Au CH Montperrin, les échanges par disquettes de données médicales à des fins statistiques, l'usage de la télécopie et du risque de mauvais acheminement.

En l'absence de contrôle rigoureux et de gestion des données, l'accès à l'information et sa diffusion sont insuffisamment contrôlables. L'accès aux données est non seulement par l'absence de maillage de l'ensemble de l'établissement mais également par les habitudes et la tradition et enfin par l'impossibilité ou la difficulté à retracer l'information.

L'informatique présente un risque de viol des données et requiert les mêmes précautions que les autres supports. Or, à Montperrin, le travail préparatoire d'observation de la transmission sur support papier a été très révélatrice et a été l'occasion de se préoccuper de la façon dont l'information est stockée, conservée, protégée et anonymée. La présidente de la CME reconnaît que la circulation papier est loin d'offrir toutes les garanties de sécurité : « le système actuel reste très faillible ; il n'est pas la panacée, mais une effraction reste circonscrite, alors qu'avec le réseau, l'effraction peut être massive ».

48% des utilisateurs du SIM estiment en effet que les données médicales partagées par le mode papier ne sont pas bien protégées[162].

Au CH Montperrin, nous verrons que les menaces ont été identifiées, au sein du rapport d'audit, en fonction de la sensibilité des données et des traitements, de l'environnement, des contraintes légales et réglementaires. Cette phase de repérage des menaces et faiblesses est en effet nécessaire pour déterminer les scénarios de risques en terme de disponibilité, d'intégrité, de confidentialité et d'auditabilité.

Au CH Montfavet, bien que n'étant pas un axe stratégique du premier schéma directeur informatique, la sécurité du système d'information mise en œuvre aussi bien en terme de confidentialité qu'en terme de disponibilité, était exprimée par les utilisateurs comme un besoin réel et était sous-entendue dans les axes de travail retenus. Un projet sécurité a donc été initié en 2001, avec la définition de la politique de sécurité de l'ensemble du système d'information. Un important chantier sécurité a été réalisé dans les années 2001-2002 avec l'aide du Comité Sécurité comprenant des représentants des principales fonctions de l'établissement puis à travers la mise en place du Comité de Veille Informatique Médicale sous l'égide de la CME. Des nombreuses opérations ont été réalisées à ce jour ou sont en projet.

Un des établissements précurseurs dans le domaine de l'informatique de santé, les Hôpitaux Universitaires de Strasbourg (HUS), a déployé un projet sécurité depuis 10 ans avec l'implantation d'un serveur sécurité en 1996, une évaluation de la sécurité et de la CPS en 1999, mais n'a pas encore mis en place de plan de secours, ni de comité de sécurité officiel. Le RSSI des HUS, interrogé travaille d'ailleurs actuellement à la formalisation d'une politique de sécurité aux côtés du CIM pour les questions d'information médicale et du GMSIH.

B) Une prise de conscience fortement conditionnée par les recommandations de l'Agence Nationale d'Accréditation et d'Evaluation en Santé (ANAES)[163]

La sécurité des systèmes d'information est étudiée dans le chapitre 4 intitulé « Gestion du système d'information (GSI). La politique de sécurité est définie par le manuel d'accréditation de l'ANAES comme un « ensemble de lois, règles et pratiques qui régissent le traitement des informations sensibles et l'utilisation des ressources d'un système d'information ou d'un produit ».

---

[162] *Cf*. annexe I

[163] *Cf*. Rapport d'activité 2003 de l'ANAES, qui fait apparaître 41 recommandations et 4 réserve dans le domaine « politique de sécurité des SI » (Référentiel GSI 1) et 95 recommandations et 5 réserves dans le domaine « confidentialité et sécurité des informations » (référentiel GSI 2)· Annexe 1 (cartographie des référentiels, recommandations et réserves…), page 35 http://www.anaes.fr

En effet, l'obligation qu'ont les établissements de soins d'évaluer leurs pratiques professionnelles[164] se traduit par le référentiel d'accréditation GSI 1 qui encadre la définition et la mise en œuvre de la politique des systèmes d'information (par exemple : amélioration de la qualité des soins par la réduction des délais d'attente, par une aide à la prise de décision, etc.).

Accrédité en novembre 2002, le CH Montperrin s'est vu opposer une réserve par le collège de l'accréditation de l'ANAES : « rendre opérationnelles les vigilances sanitaires, formaliser les procédures nécessaires, former les professionnels concernés et évaluer le dispositif », ainsi que 4 types de recommandations :

- reprendre une réflexion globale sur le dossier du patient permettant d'établir avec les professionnels les modalités de sa circulation, sa tenue, son contenu, son accès, dans un souci d'harmonisation
- impliquer davantage les instances et les professionnels dans l'actualisation du schéma directeur de l'information
- organiser une gestion documentaire
- structurer au niveau de l'établissement un programme de prévention des risques s'appuyant en particulier sur un système unique de signalement des évènements indésirables et l'évaluer.

Plus synthétiquement, l'ANAES a donc émis des remarques et des recommandations sur la protection des informations médicales nominatives, la maîtrise par les professionnels de la connaissance et de la définition du SI, l'absence d'informatique à l'usage des soignants et un cloisonnement entre les domaines applicatifs administratifs et médicaux. E. DUSEHU, expert-visiteur à l'ANAES, constate que la question de la confidentialité des données fait très souvent l'objet de recommandations.

Devant la nécessité de déployer l'informatique du CH Montperrin, il s'est avéré nécessaire de définir et de formaliser un cadre de contrôle qui instaure un équilibre entre la protection des données et la facilité d'accès des personnes autorisées. Des contraintes trop lourdes seraient détournées, un outil trop complexe serait difficilement exploitable. Si des mesures techniques spécifiques sont nécessaires, comme l'authentification des accès par mot de passe ou le chiffrement des flux, elles doivent être intégrées dans un cadre plus vaste de règles fonctionnelles et organisationnelles. C'est l'objet de la politique de sécurité.

[164] Article L. 6113-2 du Code de la santé publique.

3.1.2 Evaluation préalable et correction

A) L'audit de sécurité

Au regard des exigences normatives déjà énumérées et du retard accusé par l'établissement, il ne pouvait plus être fait l'économie d'une réflexion sur l'évaluation du niveau de risque auquel le système d'informations de l'établissement est exposé, des moyens financiers nécessaires et l'effort d'organisation inhérent à ce changement technico-organisationnel. La définition de la politique de sécurité a donné lieu, au débit de l'année 2003, à la réalisation préalable d'un audit technique et organisationnel du SIM et du SIA, ainsi qu'à la production d'un plan de recommandations actuellement en cours de mise en œuvre. L'audit a porté sur les composantes des systèmes d'information, les règles de filtrage (pare-feu), les systèmes d'exploitation des serveurs hébergeant des données sensibles, la base de données hébergeant les informations pharmaceutiques, les procédures de gestion de sécurité.

Une synthèse des forces et des faiblesses ainsi qu'une cartographie des risques ont été dégagées de cet audit. Les mesures techniques actuelles de sécurisation du SIA ont été jugées satisfaisantes. La gestion d'accès aux données par le réseau administratif se fait par mot de passe et nom d'utilisateur défini localement par l'utilisateur ; les partages d'informations avec d'autres utilisateurs sont définis par l'administrateur système et ne se font que sur les contrôleurs du domaine administratif (serveurs installés dans le service informatique) et les données ne sont donc plus stockées localement sur l'ordinateur. La protection comporte l'ensemble des mesures classiques de protection physique : contrôle des accès aux locaux, dispositifs anti-intrusion, régulation de l'alimentation électrique, protection contre l'incendie et l'inondation. La protection logique comporte des mesures d'identification, d'authentification, la possibilité de contrôle des transactions, la sauvegarde des données et des programmes, la mise en place de dispositifs antivirus, procédures de cryptage et de dispositifs anti-intrusion capables de contrôler les flux échangés avec le monde extérieur. *Les* réseaux logiques (ex. l'intranet) sont tous reliés à un pare-feu[165] (firewall en anglais), système physique (matériel) ou logique (logiciel) servant d'interface entre le réseau interne de l'hôpital et les réseaux externes (du type Internet), afin de contrôler et éventuellement bloquer la circulation des messages ou tentatives d'accès non autorisés. En revanche, il est incapable d'assurer la

[165] En cas de panne du pare-feu en production, le deuxième prend automatiquement le relais. Il a pour fonction de maintenir des personnes à l'extérieur (curieux qui génèrent du trafic, vandales qui saturent les liaisons, corrompent les données, espions qui brisent la confidentialité de l'information), de maintenir des personnes à l'intérieur (éviter la fuite d'information non contrôlée vers l'extérieur) et de contrôler les flux entre les réseaux interne et externe (observation de la consommation Internet des différents utilisateurs internes et possibilité de bloquer l'accès à certains sites contenant des informations illégales). Enfin, il simplifie la gestion de la sécurité et l'administration du réseau car il centralise les attaques potentielles.

confidentialité des données et ne protège pas des attaques dirigées vers les données (virus, chevaux de Troie…). Une fois qu'il a permis l'accès à des données, il ne peut en maintenir le contrôle. De cette manière, les messages électroniques ou mots de passes d'authentification en clair peuvent être lus pendant leur traversée du réseau. Enfin, le firewall ne prémunit pas les réseaux des techniques d'écoute ou de "sniffing". En d'autres termes, il ne peut pas remplacer l'attention et la conscience des utilisateurs qui doivent respecter un certain nombre de règles... La première étant bien évidemment de ne jamais ouvrir un fichier attaché à un mail sans être sûr de sa provenance, ou de s'assurer que chaque poste de travail dispose d'un anti-virus, mis à jour quotidiennement. Les virus passent également très facilement par disquette et par Internet ; la présidente du CIM en a récemment fait les frais : son poste de travail, qui ne comprenait heureusement pas de données médicales, ayant été infecté par près de 100 virus, dont six programmes espions. Or, les plateformes anti-virales du SIA auraient permis d'éviter cet incident, si le poste de travail du médecin avait été connecté sur le réseau. Tout message entrant ou sortant est transmis au préalable – pour analyse – aux plates-formes antivirales dédiées.

En revanche, l'audit a mis en exergue les faiblesses du SIM en particulier son isolement, la limitation de ses possibilités d'évolution et son incapacité à garantir à lui seul la confidentialité des informations qu'il héberge.

Après avoir évalué les risques, il convenait de choisir des mesures constituant une réponse proportionnée aux risques encourus : c'est l'objet du plan d'actions correctives.

B) Mise en œuvre d'un plan d'actions correctives

Nous avons été chargée d'initier, de piloter et de déterminer la stratégie à mettre en œuvre pour le niveau approprié de stratégie. Dans le cadre du CH Montperrin, il convenait de procéder progressivement, par paliers de maturité. Nous avons accompagné l'élaboration d'un plan d'actions correctives, aux côtés d'un ingénieur en informatique. A partir de la liste des faiblesses et des recommandations énoncées par le rapport d'audit, nous avons classé ces faiblesses par ordre d'importance et estimé la probabilité de leur occurrence afin de traiter en priorité les risques inacceptables. Il n'a pas en revanche été possible d'évaluer les conséquences financières et organisationnelles de chaque risque, sinon de manière globale et approximative. L'objectif premier était de répondre aux besoins de confidentialité, de disponibilité, d'intégrité et de promouvoir une approche transversale de la sécurité du système d'information. Le plan de communication choisi fut de définir la stratégie de communication à mettre en œuvre afin de garantir la participation et la mobilisation des acteurs, de préparer les interlocuteurs au changement amené par le projet (nouveaux outils, nouvelles procédures, évolution des comportements…). Comme le soulignait le président du GMSIH, Y. MORICE lors de la Journée annuelle des

adhérents 2004 du GMSIH[166], « le facteur-clé du succès du succès pour un système d'information, c'est d'entrer dans une démarche du changement ».

Au regard des cibles identifiées, des populations affectées, nous avons tenté de cerner les besoins en communication associés et de préparer des messages appropriés au travers de supports de communication informatiques (powerpoint, rétro-projection). Après un classement de chaque menace ou faiblesse au regard de sa criticité et sa faisabilité technique, financière et sur le plan des opérations – c'est à dire dans le contexte de la gestion et de la culture de l'hôpital, à l'instant T-, et une pondération des deux critères, nous avons élaboré un plan d'actions et un calendrier des interventions quelque peu ambitieux de mise en œuvre. Ce plan d'actions comprenait des actions à court terme pour supprimer les vulnérabilités les plus importantes, et des projets à moyen terme pour construire une véritable politique de sécurité.

3.2 Elaboration d'un cadre de référence propre à gagner ou à restaurer la confiance des utilisateurs

Le niveau de perception de la problématique « sécurité » à Montperrin commandait de construire un document intermédiaire, le plus évolutif possible et qui soit de nature à susciter la confiance des utilisateurs. Il est intéressant de noter que 11 %des utilisateurs du SIM et 16 % des utilisateurs du SIA considèrent le SIH comme « un réseau tentaculaire contrôlé par les seuls spécialistes » et 13 % de chaque groupe l'assimilent à « une sophistication électronique ». Nous tenterons ici de proposer les solutions techniques, fonctionnelles, organisationnelles aptes à établir une confiance univoque des utilisateurs dans leur système d'information, à partir notamment des consignes de mise en œuvre énoncées dans le référentiel validé mais aussi des pistes que nous ont ouvert les enquêtes de terrain, la lecture bibliographique et l'analyse des obstacles.

3.2.1 La rédaction d'un référentiel technico-organisationnel

Pour utiliser efficacement les technologies de sécurisation des données, il faut instaurer une discipline organisationnelle. La politique de sécurité doit être retracée dans un document cadre définissant les enjeux, les principes d'action et d'organisation ainsi que les objectifs à atteindre. La relation d'interdépendance décrite plus haut entre système d'information et organisation hospitalière nous enseigne qu'il est souhaitable d'accompagner tout changement par une redistribution des tâches, une modification de la technologie, de la structure.

[166] Qui s'est tenue le 8 juillet et consacrée au thème suivant "Le système d'information hospitalier de production des soins et le système d'information de santé : actualité et expériences".

A) L'esprit de la politique de sécurité

Basée sur la norme ISO 17799 et sur les recommandations du GMSIH, elle vise à définir l'ensemble des niveaux d'exigence de sécurité organisationnelle, juridique, humaine et technique pour mettre en cohérence les contraintes environnementales (notamment réglementaires) avec les objectifs opérationnels du futur système d'information de l'établissement. Le référentiel de sécurité est la « bible sécurité du SIH » qui décrit une réalité du CH Montperrin à un moment donné et reste un socle qui doit s'adapter à son environnement et à l'évolution de l'établissement. Tous les établissements sont loin de disposer d'un document formel et s'appuient sur le «bon sens » et « sur les politiques de sécurité reconnues de manière générale par la profession d'informaticien », comme nous le confie l'un des membres de l'équipe informatique du CH de Roubais[167], pourtant 7ème établissement français. «La CNIL favorise l'édiction de chartes internes, une prise de conscience de la sensibilité des informations nominatives, car les problèmes de communication se posent surtout dans les établissements », précise Jeanne BOSSI, Chef de Division des Affaires publiques et sociales de la CNIL[168]. Les protections techniques précédemment énumérées doivent s'inscrire dans le cadre d'une politique de sécurité de l'établissement, indispensable à la réalité de leur mise en œuvre et à leur pérennité. Cette politique de sécurité était, en 2003, encore embryonnaire et surtout non formalisée.

Dans ce contexte difficile où l'hôpital, en tant qu'organisation, et les individus poursuivent des objectifs conflictuels (liberté et sécurité, préservation et intérêts catégoriels) en partie, l'hôpital s'est pendant longtemps orienté vers des prises de décision incrémentielles, des solutions ordonnées de manière séquentielle, c'est-à-dire qui restent proches de ce qui existe déjà, dans le prolongement des politiques antérieures, ou encore des non choix qui sont en eux-même des prises de décision. Rompant avec le passé, et après moult difficultés, la politique de sécurité qui a été validée, si elle ne bouleverse pas radicalement l'organisation actuelle, est un compromis qui reflète les conflits, les groupes concernés, les intérêts, les cadres de référence et la négociation musclée qui s'est élaborée pendant près d'un an. Solution jugée « satisfaisante » par tous, elle est le résultat d'un premier stade de maturité.

B) Contrôles d'accès physiques et logiques

[167] Entretien électronique en date du 30 avril 2004.
[168] Entretien téléphonique en date du 10 septembre 2004.

Les organisations de santé ont des besoins spécifiques en matière de gestion des droits d'accès. Une première version de la politique de sécurité a été validée par le COPIL le 21 juin 2004. Elle correspond, comme nous l'avons vu à un document intermédiaire, qui n'impose pas des normes trop strictes, appelé à évoluer. Elle comprend notamment deux branches : sécurité physique des locaux et technique au travers d'une politique d'identification et d'authentification au niveau de chaque utilisateur et de chaque application.

a) Contraintes physiques

La protection physique requiert en théorie l'implantation du « cerveau » du système informatique dans une zone protégée pourvue de détecteurs anti-intrusion, fermée par une porte blindée équipée d'une serrure de sécurité ou d'un dispositif électronique. Dans la pratique quotidienne ces éléments de sécurité sont rarement réunis, comme c'est le cas à Montperrin. Ainsi, le serveur de la SMTEIM, actuellement installé sur le poste de travail de son statisticien, dans un local qui n'est pas suffisamment sécurisé, devra être rapatrié dans les locaux de l'équipe informatique, aux côtés du serveur du SIA. Ce rapatriement a été accepté par le corps médical sous réserve d'être installé dans une armoire dont l'accès reste exclusivement réservé au personnel de la SMTEIM. Au niveau du réseau, des dispositifs anti-intrusion doivent être également mis en place pour lutter contre les risques de " piratage " à distance.

b) Contrôle d'accès logique

L'établissement doit prendre les mesures nécessaires au contrôle de l'accès aux informations, que ce soit par accès aux données directement ou aux traitements et procédures opérationnelles utilisant ces données. La sécurité logique comporte soit une protection des accès par des mots de passe -option qui a été choisie au CH Montperrin – soit, ce qui est beaucoup plus performant, un dispositif de lecture de carte à microprocesseur de professionnel de santé (CPS)[169]. L'ensemble des dispositifs de sécurité logique est appelé à se renforcer compte tenu des besoins accrus en identification, authentification et chiffrement[170] nécessités par les évolutions normatives et les contraintes sécuritaires qui en découlent. Il conviendra de mieux suivre l'ensemble des incidents pouvant intervenir sur le système d'information, afin de les résoudre ou de les supprimer aux travers de procédures permettant de suivre ces incidents, leurs répercussions, les délais, la qualité des intervenants et l'efficacité des solutions proposées.

[169] Prévue à moyen ou long terme.
[170] Ou cryptage, c'est-à-dire l'encodage et le décodage des messages pour prévenir l'accès non autorisé aux données ou pour empêcher l'intrus de les comprendre.

D'autres dispositifs ont été préconisés par la société de conseil comme l'arrêt automatique du système dès qu'il n'est plus utilisé durant quelques minutes.

La politique d'autorisation[171], qui est une déclinaison de la politique de sécurité, décrit les modalités fonctionnelles et organisationnelles du contrôle d'accès et de l'attribution des droits (lien entre un utilisateur, son rôle et ses droits sur une ressource donnée en fonction d'un contexte ; règles de gestion des autorisations et de traçabilité des accès, modalités d'administration des autorisations). La politique d'autorisation s'appuie, pour autoriser l'accès à des ressources, sur les habilitations[172].

La gestion des droits d'accès devra être centralisée et cohérente au niveau de l'établissement. Actuellement, elle est peu protocolisée[173]. Une grille d'habilitation devra préciser la capacité des profils utilisateurs à pouvoir accéder, lire, écrire, signer sur des données administratives ou médicales. Les restrictions seront posées dans la même grille. Les droits d'accès aux données du Système d'Information Hospitalier seront déterminés par le responsable de chaque service en fonction des missions exercées, la supervision et contrôle de l'administration des droits d'accès restant sous la co-responsabilité du DIM et du RSSI

Pour assurer le maintien de la confidentialité, de la disponibilité et de l'intégrité des données, il conviendra d'attribuer un Identifiant et un authentifiant à chaque utilisateur, de limiter les accès aux seules informations autorisées, de générer une réinitialisation régulière des mots de passe et des sauvegardes quotidiennes, d'informer les utilisateurs sur les bonnes pratiques informatiques, qui sont autant de mesures technico-organisationnelles à mettre en œuvre.

C) La mise en œuvre opérationnelle

Dans les domaines de la gestion des droits d'accès, de l'authentification et du management de la sécurité du SI, trois procédures ont été rédigées dans le cadre de la réalisation des actions « préalables » destinées à concrétiser la politique de sécurité, et une charte de sécurité devrait être élaborée avant la fin de l'année 2004. Ces procédures doivent couvrir tout le cycle de vie des accès des utilisateurs, depuis leur enregistrement initial dans le système de contrôle d'accès jusqu'à leur annulation finale. Nous avons choisi de ne pas présenter ces procédures dans le détail, mais schématiquement sous l'angle organisationnel. Nous ferons un point également sur la maintenance-télémaintenance.

---

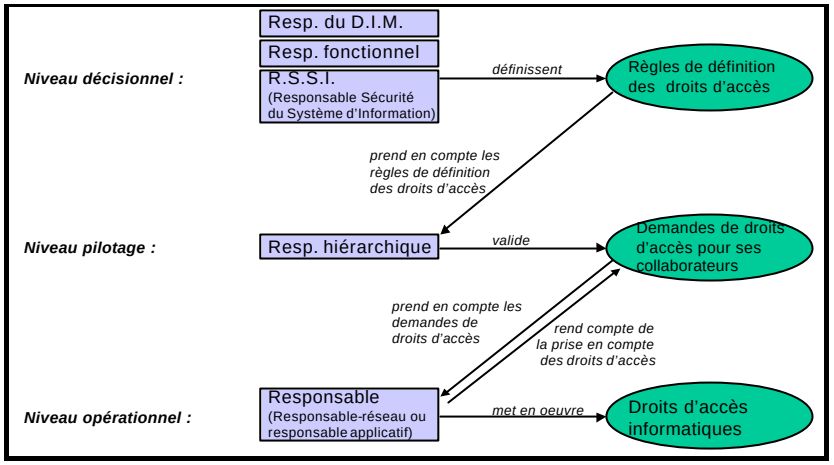
[171] Une autorisation est « l'attribution de droits, comprenant la permission d'accès sur la base de droits d'accès », source : ISO 7498-2, traduction AFNOR

[172] L'habilitation est « le droit accordé à un individu d'accéder à des informations dont le niveau de sécurité est inférieur ou égal à un niveau déterminé », source : ISO 2382-8, traduction AFNOR.

[173] Nous enjoignons notre lecteur à se reporter au A « Un quiproquo déterminant » du 2.1.2 « Dissensus ».

a) Procédure de gestion des droits d'accès

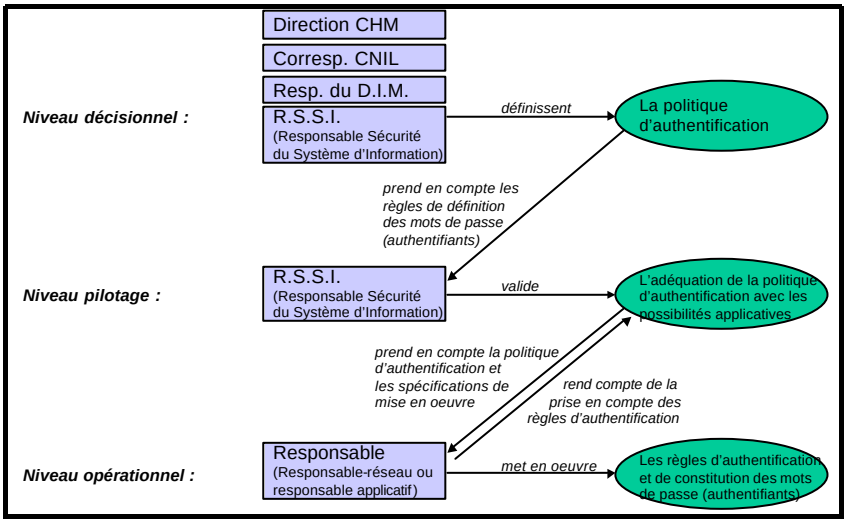
En matière de gestion des droits d'accès, le schéma organisationnel qui a été choisi au CH Montperrin est le suivant :



Nous trouvons trois niveaux (décisionnel, pilotage et opérationnel) qui correspondent à trois niveaux d'ouverture des droits d'accès (définition, validation, mise en œuvre).

b) Procédure d'authentification

En matière d'authentification, le schéma organisationnel est le suivant :



Nous retrouvons les mêmes niveaux que précédemment. A Montperrin, la politique d'authentification portera essentiellement sur la gestion des mots de passe, l'identifiant unique.

c) Maintenance, télémaintenance et confidentialité

L'hôpital doit déterminer systématiquement où se situent les données, les groupes ou individus responsables de la maintenance, de l'utilisation et de l'accès aux données,

pour chaque domaine. Il doit dès lors élaborer une politique et des règles et procédures précises pour s'assurer de l'exactitude des données, de leur sauvegarde et de leur utilisation par les personnes autorisées uniquement. La coordination des actions avec le support technique de l'application (maintenance matérielle, sauvegardes, réseau) devra être séparée des actes de soutien.

Par ailleurs, l'établissement a été amené à formaliser les procédures de sécurisation et de confidentialité avec des partenaires extérieurs. Un protocole de télémaintenance indiquant la procédure à suivre[174] a été co-signé par l'établissement et le prestataire qui assure la télémaintenance. Une clause contractuelle relative à la sécurité des traitements en cas d'opérations de maintenance ou de télémaintenance, requise par la CNIL, a également été signée. A ce titre « tous les supports informatiques comportant des données nominatives sur lesquelles doivent porter les opérations de maintenance » restent la propriété du CH, de même que pour « toutes les données dont le titulaire du contrat (de maintenance) pourrait prendre connaissance ». Il est rappelé dans cette clause que l'ensemble de ces informations nominatives[175] est « strictement couvert par le secret professionnel » et que leur traitement « doit satisfaire à l'obligation de sécurité »[176]. Est donc mise à la charge du maître du fichier une obligation de précaution. Le prestataire s'engage notamment en vertu de cette clause à « ne pas divulguer les documents et informations traités à d'autres fins que celles spécifiées au contrat », à « ne pas divulguer les documents et supports informatiques confiés à l'exception de celles nécessaires pour les besoins de la maintenance, ou encore par exemple à « prendre routes dispositions pour préserver l'intégrité des documents et fichiers (…) ». Il doit en particulier contrôler la fiabilité des matériels et des logiciels, de même que la capacité de résistance aux atteintes accidentelles ou volontaires extérieures ou intérieures en étudiant particulièrement l'implantation géographique, les conditions d'environnement, les aménagements des locaux et de leurs annexes[177]. En cas de non respect de tout ou partie des obligations énoncées dans la clause, le prestataire s'expose à la mise en jeu de sa responsabilité sur la base des articles 226-17 et s. du Code pénal[178]. Enfin une clause spécifique de confidentialité en cas de sous-traitance a été cosignée par le prestataire concerné et le CH, qui précise également, en dehors des obligations précitées,

[174] Accord préalable du CH avant chaque opération de maintenance, connexion et déconnexion du routeur, horaires d'appel et numéros de téléphone.
[175] C'est-à-dire toutes les données personnelles ou individuelles qui permettent l'identification d'une personne physique de manière directe ou indirecte par un identifiant caractérisant la personne sans la désigner nommément.
[176] La loi du 6 janvier 1978 prévoit en effet que tout responsable d'un centre de traitement de données nominatives doit prendre toutes précautions utiles afin de préserver la sécurité des informations recueillies.
[177] Recommandation n°81-94 de la CNIL du 21 juillet 1981.
[178] Article 226-17 : « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi nº 78-17 du 6janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende », *cf.* annexe II.

l'obligation du prestataire de procéder à la destruction des fichiers manuels ou informatisés, ou à restituer les supports d'informations.

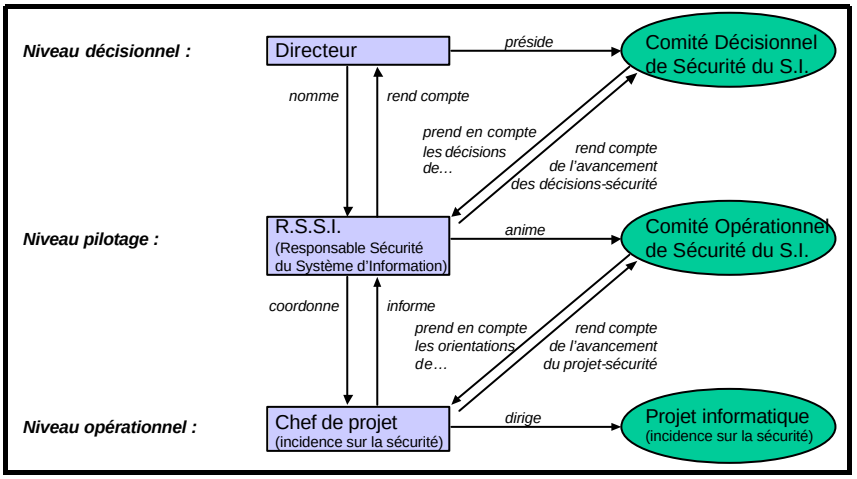
La mise en œuvre de la politique de sécurité du SII ne se limite pas à des aspects techniques, mais comprend également des changements sur le plan de la gestion, de l'organisation, des fonctions. Le CH doit anticiper et gérer les changements de comportement et d'organisation introduits par le SI sécurisé en gestation. Il ne faut pas ignorer ces changements, car ils peuvent être autant des moteurs que des inhibiteurs de l'adoption et de l'utilisation du système.

3.2.2 Changements sur le plan de la structure

Le changement doit être accompagné afin d'anticiper les évolutions futures, de susciter l'engagement de l'encadrement et des personnels, de mobiliser les équipes projet, de faciliter l'apprentissage de l'outil. L'évolution des pratiques professionnelles peut en effet engendrer des craintes et des résistances comme nous l'avons vu. Même au Centre Hospitalier de Fréjus Saint Raphaël, site pilote accompagné par le GMSIH dans l'élaboration de sa politique de sécurité, où il n'y a pas de résistance d'ordre sociologique nous confie le RSSI, « il est difficile de faire travailler les personnes sur une politique de sécurité globale, de mobiliser les utilisateurs y compris la direction »[179].

A) Gestion et organisation de la sécurité

Il convient de définir clairement les responsabilités liées au contrôle du SIH, à sa vérification et à son administration. Le schéma de management de la sécurité su CH Montperrin est le suivant :



[179] Entretien téléphonique en date du 10 mai 2004.

L'établissement doit créer un Comité Décisionnel de Sécurité du Système d'Information présidé par le Directeur de l'établissement, dont la mission est d'assister ce dernier dans la définition des orientations de la politique de sécurité. Il est probable que l'actuel COPIL sera transformé en Comité décisionnel. Un Responsable de la Sécurité du Système d'Information (RSSI) doit être identifié, dont les missions et responsabilités feront l'objet d'une fiche de poste et dont les moyens d'action sont en rapport avec les missions confiées. La création de telles instances, proposées par les référentiels généreux du GMSIH, peut paraître inadaptée à un petit CH : même le RSSI des HUS y voit une solution « irréaliste », bien qu'il est indispensable d'adapter une structure décisionnelle, et le RSSI du CHI de Fréjus « un encadrement idéaliste qui manque parfois de lisibilité ». Aux HUS, un pôle est dédié exclusivement à la sécurité, coordonné par le RSSI. Aucun responsable proprement dit de la sécurité des informations n'était formellement désigné, aucune charte utilisateur n'était conçue. Au CH Monfavet[180] par exemple, un comité de veille informatique collecte les difficultés et préoccupations des médecins concernant la confidentialité de l'outil informatique et émet des recommandations sur la transmission et la sécurité des données médicales[181].

Concernant la conduite de projet, le suivi et le contrôle, le CH Montperrin envisage de recruter un chef de projet. Ce dernier devra posséder des compétences techniques (gestion, informatique), et relationnelles (gestion de conflits, animation d'équipe, management du changement). Des effets notables sur les conditions de travail individuelles et collectives et sur la redistribution des tâches et des fonctions doivent être anticipés.

B) Incidences fonctionnelles

Bien qu'elles concernent tout utilisateur actuel ou futur du SI, nous avons choisi de n'aborder que les cas du médecin-DIM et du RSSI.

a) Le rôle du médecin-DIM

Les champs d'activité du DIM sont notamment de participer à la conception du schéma directeur de l'informatique, au recueil, au traitement, à la transmission et à la conservation des informations issues du fonctionnement des services aux fins d'analyse de l'activité de l'établissement[182]. C'est sur la base des données fournies par les

[180] Où un audit sur la sécurité informatique a été réalisé en 2002, et sera renouvelé en 2004.
[181] Par exemple, un questionnaire a été utilisé et évalué par le comité de veille informatique, avec à la clé, des recommandations sur l'utilisation des données médicales et administratives issues du système d'information.
[182] « Le médecin responsable de l'information médicale transmet à la commission ou à la conférence médicale et au directeur de l'établissement les informations nécessaires à l'analyse de l'activité, tant en ce qui concerne l'établissement dans son ensemble que chacune des structures médicales ou ce qui en tient lieu. Ces informations sont transmises systématiquement ou à la demande. Elles consistent en statistiques agrégées ou en données par patient, constituées de

praticiens et transmises par le DIM[183], que le directeur de l'établissement adresse aux services centraux et déconcentrés des ministères chargés de la sécurité sociale et de la santé et aux organismes d'assurance maladie, des statistiques de caractère non nominatif.

Avec l'informatisation des dossiers médicaux, le DIM deviendra l'administrateur, au moins officieux, du serveur des données médicales (gestion des autorisations d'accès, exploitation, maintenance…). Parallèlement au développement de l'informatisation des unités de soins, il devra conduire une réflexion éthique continue afin de garantir le respect de la confidentialité et de la protection de la vie privée ainsi que de la transparence. Il aura sinon à jouer un rôle de formation, sinon de diffusion de la culture sécurité de l'information. On peut souhaiter qu'à terme et sur accord de la CME, le médecin-DIM publie sur l'intranet de l'établissement, sous forme d'indicateurs non nominatifs, les bilans d'activité des services, ou encore, après validation par les Instances, des tableaux d'indicateurs médicalisés concernant l'établissement.

b) Le rôle du responsable de la sécurité du système d'information (RSSI)

Il a été décidé de nommer un RSSI qui ne soit ni l'administrateur réseau ni le DSIO, et de revoir à cette occasion les fiches de poste de l'équipe informatique à la lumière de la future configuration du SI, etc. Ce responsable a essentiellement un rôle de pilotage et de coordination pour la mise en œuvre, l'application et l'évolution de la politique de sécurité de l'information, qui recouvre, selon le RSSI des HUS, « les fonctions d'audit, d'évaluations périodiques, d'assistance et de conseil sur les projets »[184]. Il est le maître d'ouvrage des projets sécurité et participe à la sensibilisation des acteurs à la sécurité. Indépendamment de son rattachement hiérarchique, il dépend fonctionnellement du directeur de l'établissement, auquel il rend compte de son action.

Par délégation du directeur, il jouera un rôle majeur dans l'animation des équipes et dans la coordination des travaux opérationnels et notamment la sensibilisation du personnel aux enjeux de la sécurité, aux menaces et risques qui peuvent affecter la confidentialité des informations médicales. Le RSSI pressenti sera soit la personne actuellement responsable de la sécurité générale de l'établissement (incendie, vol…), soit l'ingénieur en organisation de la cellule qualité qui met en œuvre et suit la démarche qualité à Montperrin.

La mise en œuvre du projet de sécurisation et de déploiement du SI, en introduisant une modification des procédures, de l'organisation, des méthodes de travail,

---

telle sorte que les personnes soignées ne puissent être identifiées », décret n° 94 – 666 du 27 juillet 1994 relatif aux systèmes d'informations médicaux et à l'analyse de l'activité des établissements de santé publics et privés.

[183] dans les conditions fixées à l'article R. 710-5-8.

[184] Entretien en date du 11 mai 2004.

des outils et de l'environnement suscitera également des modifications rapides et profondes, concernant les compétences, la culture, les comportements, les valeurs qu'il sera nécessaire d'accompagner.

3.3 Accompagner les changements sur le plan de la culture, des comportements et des pratiques

Pour gérer un grand projet de transformation du système d'information, tel que la sécurisation du Si et son déploiement, la qualité de la communication est aussi pertinente que la qualité des choix technologiques et organisationnels : un grand projet est par nature transversal.

Aujourd'hui, une meilleure reconnaissance, de la part des directions générales, du rôle des technologies, la complexité grandissante des systèmes d'information, imposent d'avantage de convaincre, et donc de communiquer. La part stratégique du système d'information commence aujourd'hui à émerger : la communication est indispensable pour visibiliser le système d'information non plus comme un centre de coûts mais comme un système créateur de valeur. Elle doit faciliter un langage commun. En effet, le principal reproche fait aux consultants externes par la partie médico-soignante du COPIL, reposait sur le sentiment de se voir imposer par ces derniers un modèle entreprenarial unique et intangible au travers d'un langage technico-sibyllin. Même si le cœur du discours est commun, la forme du message doit s'adapter à la cible, à des moments privilégiés, avec des outils spécifiques (à l'occasion du COPIL, dans la lettre d'information, à l'embauche, par des lettres flash sur intranet et comme nous le verrons par la formation).

3.3.1 Informer

La réussite d'un projet impliquant des modifications passe inévitablement par la prise en compte des facteurs humains. L'établissement doit sensibiliser aux risques qui menacent l'information et le SIH, et aux moyens de s'en prémunir car la question de la sécurité n'est pas seulement une affaire de fiabilité du matériel.

A) Sensibiliser les utilisateurs en recherchant leur adhésion et leur participation

L'étude réalisée par le GMSIH en 2001 souligne que les directions appréhendent encore de manière incertaine l'importance de la sécurité des systèmes d'information. « Le problème est le manque de préoccupation des établissements de santé dans le domaine

de la sécurité informatique et de l'informatique en général, l'informatisation est disparate et inégale, la Carte de Professionnel de Santé (CPS) est encore méconnue[185]. En dehors des coûts financiers qui sont certainement un obstacle, il y a aussi un défaut de politique de sensibilisation », constate Jeanne BOSSI.

La première nécessité qui nous apparaît dans le contexte montperrinois est de banaliser l'outil informatique. La sécurité ne doit plus être perçue comme un pré-carré technique.

Il est également indispensable d'identifier les enjeux et les différents acteurs, avec une clarification du rôle de chacun (Direction, DSIO, CIM, SMTEIM, consultants externes, COPIL…). Les messages devront être adaptés aux cibles concernées, afin que les actions menées en direction des différentes cibles soient hiérarchisées et planifiées. A ce stade nous ne disposons pas de suffisamment d'éléments pour proposer un chiffrage et une évaluation budgétaire des actions de communications à mener, mais la stratégie de communication doit, selon nous, rester simple : communiquer sur ce qui a été fait, ce qui fonctionne, et ce qui doit être réalisé à court terme.

L'innovation, pour qu'elle soit bien reçue, acceptée, doit selon nous être soutenue par les cadres supérieurs (Direction, DSIO, Chefs de services) et par la base (les utilisateurs). C'est un vrai défi de faire comprendre l'importance de la politique de sécurité du système d'information aux gestionnaires qui sont hors des circuits des SI et à l'ensemble du personnel hospitalier. La DSIO aura également à relever le défi de l'estimation du temps et des coûts à investir et de la complexité : l'élaboration échelonnée sur plusieurs années, complexité des projets de très grande envergure.

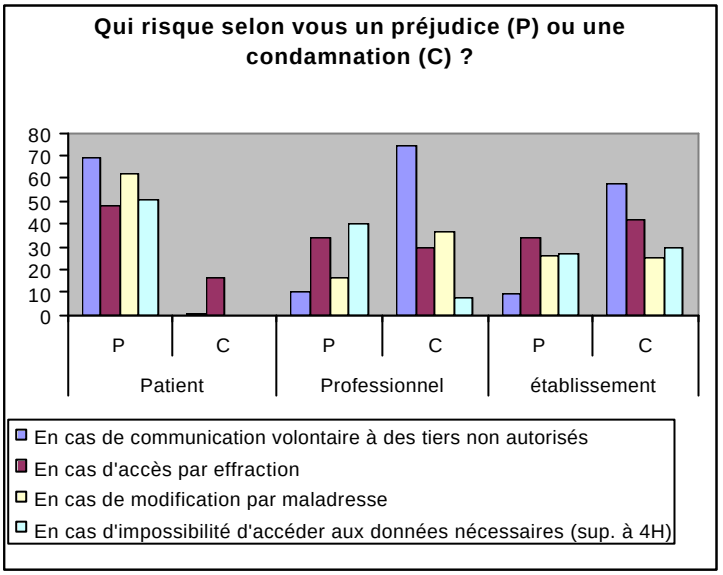
Les agents du changement sont également très importants : en l'occurrence, c'est le DSIO qui a joué le rôle de catalyseur principal, soutenue par les autres directeurs adjoints, quelques médecins et soignants, la pharmacienne, et l'équipe informatique.

Un système d'information ne peut être imposé à ses utilisateurs, il doit convaincre, être utile pour que les personnes intéressées puissent adhérer aux nouveaux principes et conditions de travail. L'assistance aux utilisateurs est donc très importante et suppose une disponibilité importante ; elle peut revêtir plusieurs formes : accompagnement sur le terrain, assistance en ligne, réseau de correspondants, procédure de traitement des anomalies rencontrées lors du démarrage. Il serait souhaitable qu'une information soit dispensée à chaque nouvel utilisateur, de manière adaptée selon qu'il s'agit d'informatique médicale ou administrative. Le DIM pourrait avoir en charge l'élaboration et la diffusion d'un document à l'attention des utilisateurs du médical. La responsabilisation

[185] Cette méconnaissance a été confirmée lors de l'exploitation des questionnaires : près des trois-quarts des professionnels de santé ne savaient pas ce que signifiait « CPS ».

passera également par l'usage de la signature électronique, lorsque la CPS sera déployée sur l'établissement.

Les solutions techniques ne sont efficaces que si elles sont accompagnées d'un important effort de sensibilisation des personnels sur la confidentialité, notamment sur les sanctions, en particulier pénales, encourues en cas de divulgation de manière directe ou indirecte, volontairement ou involontairement, au secret professionnel[186] ou aux droits de la personne[187]. 78% des utilisateurs du SIM considèrent que la communication de données médicales entre professionnels de santé, en dehors d'un cadre précisé par la loi peut être sanctionnée.



Il est à noter que la communication volontaire à des utilisateurs non autorisés est perçue comme la principale source de préjudice pour le patient et de condamnation pour le professionnel en premier lieu et pour l'établissement. La loi du 6 août 2004 modifiant la loi informatique et libertés durcit considérablement les sanctions[188]. La législation qui entoure le secret professionnel, est encore mal connue par les professionnels de santé (en particulier des soignants). En effet, seulement 26 % envisagent la peine d'emprisonnement au titre des sanctions encourues en cas d'infraction à cette législation[189]

B) La future charte utilisateur, timide ou généreuse ?

---

[186] *Cf.* Article 226-13, annexe II.
[187] *Cf.* Article 226-21, annexe II.
[188] *Cf.* articles 226-16 226-22 du Code pénal tels que modifié par la loi n°8004-801 précitée, annexe II. Mettre en œuvre un traitement automatisé sans respecter les formalités préalables est puni de cinq ans d'emprisonnement (contre trois auparavant) et de 300 000 euros d'amende (contre 45 000) ; la divulgation d'une information susceptible de porter un préjudice est punie de cinq ans d'emprisonnement (contre un an auparavant) et de 300 000 euros d'amende (contre 15 000). Elle est punie de trois ans d'emprisonnement (nouveauté) et de 100 000 euros d'amende (contre 7 500) lorsqu'elle a été commise par imprudence ou négligence.
[189] *Cf.* annexe I.

Son objectif est de sensibiliser, d'associer et de responsabiliser chaque utilisateur en définissant les règles à respecter pour le « bon usage » des moyens informatiques et techniques mis à sa disposition dans le cadre de son exercice professionnel, dans un souci de garantir la confidentialité, l'intégrité et la disponibilité du système d'information. Après validation par les instances habilitées du CH Montperrin, la charte utilisateurs devra faire l'objet d'une diffusion formelle auprès des utilisateurs.

La facilité avec laquelle les agents pourront communiquer, recopier ou manipuler l'information sous le couvert de l'anonymat au sein d'environnements en ligne, commande de revisiter les règles traditionnelles de bonne conduite. La charte présentera des dispositions d'ordre légal, des règles d'application internes nécessaires pour induire un état d'esprit et a vocation à faire prendre conscience des responsabilités professionnelles et juridiques qui incombent à tout utilisateur dans le cadre de ses activités à l'hôpital.

Cette charte sera réalisée avant la fin de l'année 2004 par le cabinet d'audit. Nous nous sommes donc renseignée auprès de cette société mais aussi et surtout auprès des établissements de santé -de la région et de ceux qui étaient précurseurs en la matière- disposant d'une charte de sécurité afin de présenter les orientations essentielles que la charte devrait contenir. L'établissement psychiatrique voisin, le CH Montfavet, fournit en particulier des éléments intéressants au travers de sa charte de sécurité et de sa charte de « bonne conduite » du service informatique présentées aux instances d'avril 2002, modifiées et validées au cours du premier trimestre 2003. Par ailleurs, un document support résumant les règles édictées dans la charte a été élaboré, afin d'être diffusé en parallèle des deux chartes. Ces dernières sont communiquées à l'ensemble du personnel et à tout nouvel arrivant, sans toutefois être signées, en raison d'une opposition des syndicats.

Au vu des chartes élaborées dans les établissements de comparaison, nous avons retenu quelques axes principaux : la charte utilisateur doit entraîner l'adhésion et la participation des personnels et a vocation par ailleurs à faire prendre conscience des responsabilités professionnelles et juridiques qui incombent à tout utilisateur de l'informatique et s'appliquera à tout agent, titulaire ou contractuel, utilisant les moyens informatiques et internet. En face de notre public disparate d'utilisateurs avertis- réticents, amateurs-enthousiastes, novices-sceptiques et «têtes brulées », il apparaît difficile de rédiger une charte trop contraignante, au moins dans un premier temps. Les acteurs les plus opposés au projet de sécurité informatique sont les plus demandeurs de garde-fous. Il faudra au moins qu'elle précise qu'en cas de non respect de dispositions énoncées dans la charte, l'agent pourra rencontrer un simple rappel à l'ordre, la suspension du compte d'accès ou sa restriction, une sanction disciplinaire, voire une sanction pénale.

Il nous semble opportun que la future charte de sécurité réponde à ces impératifs et soit intégrée dans le règlement intérieur comme c'est le cas aux HUS[190]. La question de savoir s'il est pertinent de faire signer cette charte par chaque utilisateur, notamment à l'embauche est posée actuellement au CH Montperrin. La charte d'accès au SIH des HUS, qui inclut la charte de communication de l'information médicale, n'est plus signée depuis qu'elle est intégrée au règlement intérieur, et remise pour information lors des formalités d'embauche, comme nous l'indique le DIM G. NISAND[191]. Cela dit, bien qu'elle soit opposable par ce biais là au personnel de l'établissement, il est évidemment plus sensibilisateur de la porter à la connaissance concrète de l'utilisateur en requérant son approbation écrite. Le RSSI de Strasbourg reconnaît d'ailleurs qu'elle est moins connue depuis qu'elle n'est plus signée, c'est la raison pour laquelle elle a été rendue accessible sur le site intranet. Enfin, il est à noter que le règlement intérieur des HUS encadre également les modalités d'utilisation de la CPS (contrat de bon usage avec le GIP-CPS)[192]. Enfin, il peut être envisagé, comme au Centre Hospitalier Intercommunal de Fréjus Saint Raphaël, site pilote choisi par le GMSIH pour l'élaboration de la politique de sécurité, que la sensibilisation soit réalisée lors du recrutement par le biais du livret d'accueil et pour le personnel en place par le biais de notes de service ou d'information ou tout autre média pertinent (journal interne, référent dans le service, etc.). Mais comme le précise le RSSI de cet établissement, P. MILHON, « il n'y a pas de difficulté d'ordre sociologique… »[193].

Ces modifications peuvent induire chez l'individu des énergies, des espoirs des attentes ou des réticences ou que le chef de projet, dont le poste devrait être créé l'année prochaine, devra percevoir afin de réduire en particulier les résistances et d'utiliser les appuis.

3.3.2 Former et évaluer

« Le management des systèmes d'information est aussi indispensable à la pérennité d'un hôpital que le management des hommes » constatait P. PEYRET quelques années de cela[194]. Cette assertion est aujourd'hui d'autant plus vraie qu'il faut à la fois repenser la technologie afin qu'elle réponde aux besoins de l'organisation et des individus et modifier la structure hospitalière et l'attitude des membres par la formation, l'apprentissage.

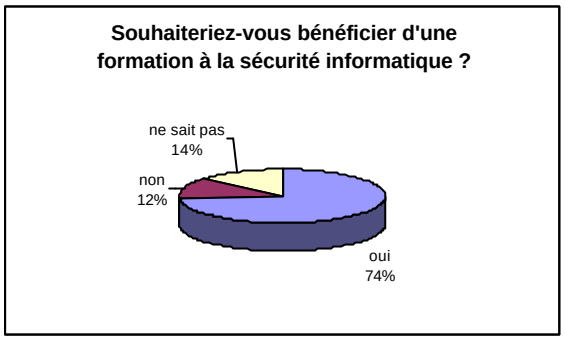
---

[190] En l'occurrence, le règlement intérieur comprend une charte utilisateur et une charte de communication.
[191] Entretien électronique en date du 7 mai 2004.
[192] A titre d'information, les Hus comprennent plus de 5 000 utilisateurs de la CPS.
[193] Entretien téléphonique en date du 10 mai 2004.
[194] dans la préface de l'ouvrage de G. PONCON, *Le Management du système d'information hospitalier*, *op. cit.*, p. 5.

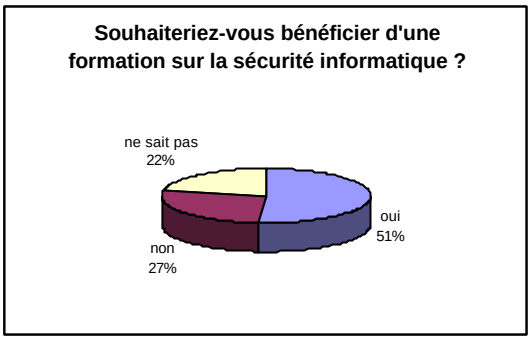
A) Mettre en place un plan de formation

Qu'il s'agisse d'erreurs ou de fraudes, l'utilisation est au cœur de la sécurité et les utilisateurs, en particuliers du SIM, semblent demandeurs de formation.

SIA



SIM



Ces résultats sont à reliés avec ceux relatifs au niveau de connaissance en matière de sécurité informatique : seulement 9% des utilisateurs du SIM le considère « très bon », contre 23 % des utilisateurs du SIA[195]. Néanmoins, ces derniers sont 54 % à communiquer « parfois » leur mot de passe à un collègue, 66 % à abandonner « parfois » ou « souvent » leur poste de travail sans le déconnecter et 35 % à ouvrir occasionnellement un fichier attaché à un mail sans être sûr de sa provenance.

Tous les acteurs interrogés ont souligné l'importance de la formation du personnel : présidente du CIM, DSIO, Informaticiens, utilisateurs. L'administrateur réseau souligne en effet qu'il « y a un gros travail de formation à réaliser, formation qui devra être adaptée au personnel de Montperrin dont l'âge moyen environne les 45 ans (…) Le gros problème, c'est déjà de les sensibiliser à respecter la politique des mots de passe, ce qui impliquera de rompre avec l'usage du *post-it* ». Avec le développement des applications informatiques, la mise en œuvre du réseau local, le déploiement de postes de travail, les besoins d'assistance aux utilisateurs seront accrus. Le RSSI[196] des HUS, reconnaît, que s'il n'existe pas d'obstacles sociologiques au développement d'un SII sécurisé, la difficulté réside dans le niveau initial de formation des utilisateurs : il est difficile de leur parler de sécurité alors qu'il ne maîtrisent pas le béaba, c'est une gageure ». Le projet d'établissement en cours d'élaboration offrira une bonne part à la question de la formation, comme c'est le cas au CH Valvert, dont le projet d'établissement 2005-2009 prévoit la poursuite des actions de sensibilisation du personnel à la confidentialité, à la sécurité des informations et la mise en œuvre d'actions de formation adaptées.

[195] *Cf.* annexe I.
[196] Entretien en date du 11 mai 2004, avec le RSSI des HUS, T. RIVAT.

Le DSIO du CH E. Toulouse a longuement insisté sur l'importance de la sensibilisation : « le projet sécurité mis en place en 2004 dans notre établissement donne une part importante à la sensibilisation et à la formation des personnels qui manquent de vision globale. La charte de sécurité sera un des médias de notre plan de communication. Elle sera annexée au contrat de travail et devra être signée. La continuité du service hospitalier justifie quelques petits effets collatéraux… »[197]. « Chaque agent à son poste de travail doit être reconnu comme partie prenante du mouvement continu de migration d'un état stable vers un autre état stable, mouvement qui caractérise tout processus de conduite du changement », souligne G. PONCON.[198]

Le DIM, celui-la même qui était si réservé sur le projet de développement et de sécurisation du SI, n'hésite pas à dénoncer le manque de formation des secrétaires médicales en informatique, «parce qu'il n'y a jamais eu de politique de formation en informatique des secrétaires, qui sont pourtant très demandeuses, comme les infirmiers et les médecins ». Après vérification, des formations en informatique ont été proposées, mais il semble qu'elles ne soient pas très fréquentées, les chefs de service ne souhaitant pas être déshabillés de leur secrétariat, qui est chroniquement en sous effectif…

Un autre problème soulevé par le DIM nous paraît essentiel : « les secrétaires saisissent de façon artistique » nous dit-il. On peut aisément supposer qu'avec la décentralisation de l'informatique dans les unités, la saisie par les soignants et les médecins reste également « artistique », en l'absence de formation adaptée. Or le SI ne pourra répondre aux objectifs qui lui sont assignés si et seulement si, en amont, la saisie est réalisée dans les règles de l'art. Il regrette que les cadres, à quelques rares exceptions, n'aient pas été équipés d'ores et déjà d'ordinateurs, « pour exorciser leur peur de l'informatique ». Un cadre interrogé sur la question qui dispose pourtant d'un poste de travail reconnaît : « On a l'impression d'être en dehors du temps, nous demandons depuis longtemps l'informatisation notamment pour être reliés avec la pharmacie. Il me semble que ce serait un gain de temps alors qu'à l'heure actuelle les soignants ne consignent pas tous les actes par manque de temps »[199]. Elle précise également que le message ne passe pas au niveau de sa hiérarchie. Questionné sur ce blocage du circuit de l'information, le Directeur des soins affirme pourtant ne pas avoir été destinataire d'une demande généralisée de postes de travail par les cadres. Il précise d'ailleurs « la demande d'informatisation émane d'une façon magique, sans être formalisée ».

Le plan de formation doit être initié au plus tôt, puis enrichi au fur et à mesure de l'avancement du projet. Il doit porter d'une part pour les « novices » sur une initiation à l'utilisation de l'informatique et d'autre part pour les utilisateurs expérimentés sur les

[197] Entretien en date du 5 mai 2004.
[198] *Le Management du système d'information hospitalier*, *op. cit.*, p. 159.
[199] Entretien avec un cadre supérieur de santé, en date du 23 juillet 2004.

mesures de sécurité à respecter. Compte tenu des besoins constatés de formation et de responsabilisation, un premier projet de formation pourrait concerner, d'abord, les secrétariats médicaux et les personnels administratifs, puis le corps médical et le personnel soignant. Il conviendra ensuite de définir des groupes homogènes pour des sessions de formations bien ciblées, des axes prioritaires de formation. Il serait opportun que cette dernière soit accompagnée par une documentation pratique (fiches problèmes).

Cette formation devra rester fonctionnelle et pratique. Aux HUS par exemple, des formations sont organisées pour tout nouvel agent ou médecin sur la confidentialité, l'usage du système d'information et la CPS. Par ailleurs, il a été choisi de sensibiliser les corps de métiers les plus concernés dans un premier temps : les secrétaires médicales se sont vues proposer cinq modules de trois heures sur l'année présentant notamment la question de la confidentialité autour des enjeux théoriques, des risques en particulier juridiques, des exercices pratiques (sauvegardes sur disques durs, etc.). La formation a été très bien reçue par les secrétariats médicaux a pu constater le RSSI. Ce plan de formation devra définir, en particulier, les supports de formation adaptés, l'organisation des sessions de formation, l'assistance aux utilisateurs lors du démarrage de la mise en oeuvre. On peut imaginer qu'à court terme la formation à l'utilisation idoine de l'informatique, l'apprentissage de la saisie des données par les personnels et l'imprégnation des règles de sécurité ne procureront pas d'avantage visible. Elle devra tenir compte de la progression. Dans l'absolu, elle devrait précéder la mise à disposition du poste de travail, et succéder immédiatement à la phase opérationnelle de démarrage. Elle devra tenir compte de la disponibilité des acteurs, et en particulier de leurs horaires décalés (cas des soignants). La présidente du CIM s'inquiète du temps soignant qu'il sera nécessaire de dégager à court terme, alors que les effectifs sont déjà insuffisants, et craint leur déception dans cette première phase lourde de formation et de tâtonnement. En revanche, elle subodore qu'à long terme, les effets positifs se feront sentir au quotidien. Les contraintes de formation seront importantes compte tenu de l'éparpillement des unités, du peu de disponibilité des utilisateurs et de leur manque d'expérience informatique. Il est souhaitable que les personnels formateurs aient une connaissance réelle du terrain et pratiquent le même langage que les utilisateurs et que la sensibilisation aux notions de confidentialité soit réalisée en collaboration avec le médecin responsable DIM et la DSIO comme cela a été fait HUS. Des formations y ont notamment été proposées autour de trois grands thèmes : la confidentialité, le SIH en général et la CPS. Enfin, il nous semble essentiel que les gestionnaires suivent également des séances de formation sur la sécurité des systèmes d'information[200].

[200] Comme c'est le cas par exemple à la First Union Corporation, sixième plus grande banque des Etats–Unis.

La culture informatique ne pourra être diffusée que dans un second temps. Il est intéressant de citer les propos du Professeur Bernard GLORION, alors Président de l'Ordre National des Médecins, tenus le 1er octobre 1997 « il faudra au moins une génération pour implanter la culture informatique dans le corps médical ».

3.3.2.1 Mesurer l'efficacité de actions menées

La mesure de l'efficacité des actions menées doit se faire tout au long du déroulement du projet et après. Une identification et une communication des benchmarks effectués, des nouveaux outils utilisés, des meilleures pratiques reconnues, mais aussi des erreurs à ne pas renouveler, doivent être organisées en faveur des projets existants ou à venir dans un souci d'amélioration d'efficacité. Les actions menées devraient entraîner une chute de la sinistralité, et générer corrélativement un gain qualitatif et financier.

Par ailleurs, la politique de sécurité de l'information doit être articulée avec la qualité et la gestion des risques, ce qui recommande de mesurer régulièrement la qualité de la sécurité de l'information et d'intégrer dans le cadre des vigilances instaurées par l'établissement, la vigilance sur la sécurité du SI (alerte et processus de réaction). Une évaluation périodique des risques reste nécessaire, notamment lors de changement dans les besoins et les priorités de l'établissement.

Après quelques temps, il sera souhaitable de mesurer l'efficacité de ces actions au travers d'une enquête sur ces actions de sensibilisation, laquelle devrait être renouvelée régulièrement. Suivant les résultats de cette enquête, un groupe de travail pourra être mis en œuvre afin d'étudier le rapport coût-qualité-performance des améliorations constatées.

A terme, pour mesurer le succès de la sécurisation du système d'information, il conviendra de mesurer le niveau d'utilisation du système, la satisfaction de l'utilisateur, l'atteinte des objectifs, les gains qualitatifs et financiers. L'évaluation plus générale de la qualité du service rendu par le SIH supposera la mise en place d'outils de mesure de la qualité sur les nouveaux projets, un suivi des incidents informatiques et de la satisfaction des utilisateurs. Dans les six mois suivant l'adoption définitive de la politique de sécurité, il est d'ores et déjà prévue la réalisation par le cabinet d'audit d'une journée «d'audit flash » dont l'objectif sera de s'assurer de la mise en œuvre effective de la politique de sécurité et d'évaluer ses éventuels dysfonctionnements, pour produire des constats et des recommandations dont le CH conservera la maîtrise.

CONCLUSION

Organisation « à buts et à agents multiples »[201], l'hôpital est par essence multifonctionnel et poursuit des objectifs qui peuvent être complémentaires ou contradictoires. Dans le premier cas, une interdépendance harmonieuse des missions favorise le dynamisme et l'adaptation ; dans le second cas, la diversité des buts suscite des conflits, des tensions et des blocages.

L'élaboration d'une politique de sécurité informatique, instrument qui accompagne la mise en place d'un système d'information généralisé à l'ensemble de l'établissement, a cristallisé ces conflits, tensions et blocages, par les problèmes d'éthique, de confidentialité et de sécurité qu'il soulève. Rien de moins surprenant car l'hôpital psychiatrique constitue un terrain privilégié où les enjeux – imaginaires aussi bien que réels – d'une telle révolution dans la gestion humaine, économique et technique de l'hôpital en général semblent se poser plus profondément qu'ailleurs. Ces enjeux, leurs origines et leurs conséquences, y sont par conséquent plus visibles et donc plus aisément décelables.

Dans un contexte, où l'argument de la protection de la confidentialité l'a longtemps emporté sur le déploiement de l'informatique médicale, l'articulation entre système d'information et secret médical/secret partagé, n'est pas chose aisée car d'une part elle croise les droits des patients, les obligations déontologiques des professionnels de santé et les exigences de transparence administrative et d'autre part elle remet en cause l'équilibre entre ces droits, les privilèges, les obligations et les responsabilités.

Les impacts d'un tel projet, conçu initialement seulement comme un outil de perfectionnement du SIH, concernent autant l'organisation que les procédures, la distribution des rôles, la gestion des ressources humaines, la culture, les comportements, les métiers, les savoir-faire, les outils et les conditions de travail. Un tel projet appelle donc un changement technico-organisationnel : la sécurité du SI est au cœur du développement de l'économie et permet de penser le service public hospitalier comme une entité traversée par des logiques organisationnelles, individuelles, éthiques, contingentes et interdépendantes. Il existe en effet une interdépendance entre d'une part les moyens techniques et d'autre part la stratégie globale de l'hôpital, les règles et les procédures. Toute modification entrant dans le champ de l'un des deux domaines supposera de repenser l'autre domaine. La notion d'efficacité ne nous paraît pas antinomique de celle de service public hospitalier. Pour en tirer pleinement profit, l'hôpital doit soigneusement planifier et gérer le changement apporté. La sécurisation du SI est une manière de le repenser, de le faire évoluer et de le

[201] MINTZBERG H., *Le Pouvoir dans les Organisations* , Les Editions d'Organisation, Paris, 1986, pp. 53-55.

transformer : le SI cible échouera si sa conception n'est pas compatible avec la structure, la culture et les objectifs de l'établissement. Le cadre de direction doit dès lors aborder les questions de la répartition des tâches et fonctions, de l'exercice du pouvoir et la culture de l'organisation.

Mais la démarche initiée ne peut qu'être progressive car elle rencontre, comme nous l'avons vu, de nombreux obstacles structurels et conjoncturels. Les difficultés s'accentuent lorsque l'on touche aux données médicales qui disposent d'un langage propre.

Concevoir une politique de sécurité du SI sur un sol quasiment vierge requiert une évolution des pratiques professionnelles et des pratiques médicales, or les individus conservent toujours une marge d'autonomie et de résistance, d'autant plus forte que le projet considéré est incontournable. Derrière la persistante résistance médicale à partager l'information concernant les patients, se cache la peur de la levée du secret, la peur de l'intrusion, voire celle, non avouée, du jugement des pratiques médicales. La sécurité est pourtant essentielle pour instaurer un climat de confiance qui favorise l'échange et le partage de données de santé à caractère personnel, mais aussi pour garantir la confidentialité, faire prendre conscience aux établissements des impacts et des enjeux de l'informatique hospitalière. C'est dans cette perspective que la politique de sécurité informatique pourra être cohérente et s'insérer de façon harmonieuse dans la politique de gestion des risques et de démarche qualité de l'établissement. La maîtrise du système d'information hospitalier est en effet essentielle pour garantir la qualité des soins, la sécurité des patients, pour faciliter la gestion interne et externe, ainsi que pour assurer des fonctions de pilotage et d'aide à la décision.

Cette même politique de sécurité appelle aussi et surtout une révolution culturelle. Il n'y a plus d'obstacles techniques ou juridiques à l'institution d'un SIH intégré et sécurisé, à la création d'un dossier unique patient informatisé ; en revanche, les obstacles sociologiques, restent comme nous l'avons vu, très présents.

« L'informatique hospitalière doit effectuer une véritable mutation » énonce le Pr Marius FIESCHI dans son rapport sur les données du patient partagées[202]. Pour permettre l'échange permanent des informations, les systèmes d'information des établissements vont devenir totalement communicants. Aujourd'hui, les établissements et les professionnels de santé doivent coopérer afin d'assurer une prise en charge des patients, pluridisciplinaire et transversale, de nature à faire évoluer les pratiques médicales vers une médecine davantage coordonnée autour du patient, permettant de simplifier et d'optimiser le parcours de celui-ci dans le système de soins. Or cette démarche à l'hôpital est d'abord la

[202] *Les données du patient partagées*, *op. cit.*

conséquence d'une exigence éthique de réflexion collective multiprofessionnelle et de consensus. C'est ce que certains nomment l'infoéthique : s'appuyer sur la dimension humaine pour susciter la confiance et construire les SIH de demain[203].

[203] Terme utilisé par INGRAND P. FESSLER J.-M., GREMY F., Les facteurs humains, incontournables conditions de succès pour les SIH de demain, *Revue hospitalière de France*, novembre-décembre 2001, n°483, pp. 46-61.

Bibliographie

Ouvrages

- CROZIER M., et FRIEDBERG E., *L'acteur et le système*, Ed. du Seuil, 1977

- LAMERE J.M., *Sécurité des systèmes d'information*, Paris, Dunod, 1991.

- LAUDON K. C., LAUDON J.P., adapt. LINGRAS L., *Les systèmes d'information de gestion*, Editions Village mondial, Pearson Education, Paris, 2001, 784 p.

- MINTZBERG H., *Le Pouvoir dans les Organisations*, Les Editions d'Organisation, Paris, 1986.

- PONCHON F., *Le secret professionnel à l'hôpital et l'information du malade*, Ed. Berger-Levrault, Paris, 1998, 233 p.

- PONCON G., *Le management du système d'information hospitalier, la fin de la dictature technologique*, Ed. ENSP, 2000, 254 p.

Revues

- CIRRE P., Le développement des technologies de l'information dans les établissements de santé, *Echanges Santé-social*, décembre 2000, n°100, pp.59-62

- HANNSKE H.-A., LEFEBVRE M., Management et communication dans l'hôpital ; un secteur à ne pas négliger : le système d'information hospitalier, *Gestions hospitalières*, avril 2000, n° 395.

- INGRAND P. FESSLER J.-M., GREMY F., Les facteurs humains, incontournables conditions de succès pour les SIH de demain, *Revue hospitalière de France*, novembre-décembre 2001, n°483, pp. 46-61.

- JONCOUR M., Produire de la valeur, *DH magazine*, mai-juin 2004, n°95.

- NAIDITCH M., POUVORVILLE G. de, Le Programme de Médicalisation des Systèmes d'information : une expérience sociale limitée pour une innovation majeure du management hospitalier, *Revue Française des Affaires Sociales*, n°1, janvier-mars 2000, pp. 59- 91

- QUANTIN C., ALLAERT F.-A., DUSSERRE L., «L'anonymat des information médicales existe-t-il ?, *Gestions hospitalières*, n°392, janvier 2000.

- RAY J. E., NTIC et nouveaux systèmes d'exploitation, *Liaisons Sociales*, juin 2004, n° 5, pp. 66-67.

- STACCINI P., QUARANTA J. F., La démarche utilisateur au centre de la conception des systèmes d'information hospitaliers, *Techniques hospitalières*, avril 2000, n°645, p. 47-51

- STEUDLER F., Le management hospitalier de demain, approche sociologique, *Revue Hospitalière de France*, n°497, mars-avril 2004.

- WAGUENAAR G., Informatique médicale et PMSI, *Le journal de Nervure*, mai 2000, n°4.

- Dossier Informatique, *Horizon*, n°150, mars-avril 2004, p. 36 et 38.

- La sécurité des systèmes d'information informatiques, *Gestions hospitalières*, n° 365, décembre1997.

- *Les systèmes d'information, des enjeux stratégiques*, La sécurité des systèmes d'information, *Echanges Santé Social*, décembre 1997-mars 1998, n°88-89, pp. 107-113.

- *Perspectives* (lettre d'information des adhérents du GMSIH), n°7, septembre 2002 ; n°9, mars 2003 ; n°10, juin 2003 ; n°11, septembre 2003 ; n° 12, janvier 2004.

- Où en est l'informatique hospitalière (Interview de J.M. AMAR, chirurgien), *Décision Santé*, mai 1997, n°113, p. 23-25.

- De nouveaux droits pour les malades, *Actualités Sociales Hebdomadaires*, 17 mai 2002, n°2262-2263, pp.37-46.

Journaux

- GEKIERE C., MORVAN O., Du dossier patient aux « données du patient partagées », *Le concours médical*, 30 juin 2004, Tome 126-24, pp. 1409-1411.

- Le Dr Michel Ducloux : une extrême vigilance s'impose, *Le Quotidien du médecin*, n° 7568, p. 3.

- Informatique médicale et PMSI, *Le journal de Nervure*, n°4, mai 2000, p.6-7.

Conférences et congrès

- *Le dossier médical : enjeu de transparence et de qualité des soins*. Quel cahier des charges, Conférence inaugurale du MEDEC, Paris, 12 mars 2002

- *Les enjeux de l'informatique de santé*, CNOM, 6ème jeudi de l'Ordre, Paris, 3 février 2000. Disponible sur Internet : http://www.conseilnational.medecin.fr/?url=colloque/article.php&offset=5

- *La place du secret entre transparence et éthique professionnelle*, CNOM, 1er jeudi de l'Ordre, Paris, 1 octobre 1998. Disponible sur Internet :

http://www.conseil-national.medecin.fr/?url=colloque/article.php&offset=0

- *Socialisation de la technique, technicisation de la société : quelle(s) sociologie(s) ? Propositions pour une analyse critique des usages sociaux des technologies de l'information et de la communication*, Groupe de travail n°13, 17ème congrès international des sociologues de langue française, Tours, 5-9 juillet 2004

Rapports

- CNIL, 23ème rapport d'activité 2002, chapitre 6, La circulation des données de santé.

- CNIL, *Santé, Informatique et Libertés – Professions libérales*, mars 1999.

Sites WEB de référence

http://www.ssi.gouv.fr

http://www.clusif.asso.fr

http://www.afnor.fr

http://www.cenorm.be

http://www.ordmed.org

http://gmsih.fr

http://www.cnil.fr

http://www.sante.gouv.fr

Liste des annexes

ANNEXE I : RESULTATS DE L'ENQUETE STATISTIQUE

Objectif de l'étude

Apprécier la représentation qu'ont les utilisateurs actuels et futur du système d'information hospitalier actuel (administratif, médical) et du système cible) et évaluer leur ressenti et leur niveau de connaissance par rapport aux bonnes pratiques de sécurité.

Méthode

L'échantillonnage réalisé est le suivant :

- Tous les utilisateurs de l'informatique administrative

- un échantillon représentatif des utilisateurs actuels et futurs du SI cible : trois services pilotes de l'informatisation et trois services non pilotes. Deux types de questionnaires fermés (« A » pour le groupe d'utilisateurs du système d'information médical et « B » pour le groupe d'utilisateurs du système d'information administratif) ont été diffusés, uniquement en intra-hospitalier. 300 questionnaires ont été diffusés ; ils ont été anonymés lors de l'exploitation. Compte tenu de la nature « sensible » du domaine d'étude au sein de l'établissement, nous ne nous attendions à un très faible retour de la part des utilisateurs du système d'information médical, or le taux global de retour (les deux groupes confondus) a tout de même été de 48 %.

Les commentaires des questionnaires remplis ou non ont été lus avec attention dans la mesure où ils apportent un complément d'information qualitatif qui est parfaitement complémentaire à l'approche statistique qui suit.

Questionnaire A (médecins, secrétaires, paramédicaux, médico-techniques, …)

Données personnelles

Nom : (les questionnaires seront anonymés lors de l'exploitation)

Vous êtes :
Un homme☐ Une femme☐

Secteur :
G17☐ G18☐ G19☐ G22☐ I08☐ Alcoologie☐
Pharmacie☐
Autre :

A quel métier appartenez vous :
Administratif☐ Médecin☐ Cadre☐ Infirmier☐
Aide-soignante☐ Médico-technique☐ Assistante-sociale ☐
Psychologue☐ Autre☐ préciser :

Votre ancienneté dans le Centre Hospitalier Montperrin :
Est inférieure à 1 an ☐ Est supérieure à 1 an et inférieure à 5 ans☐
Est supérieure à 5 ans et inférieure à 10 ans ☐ Est supérieure à 10 ans☐

Vous avez :
Moins de trente ans☐ Plus de trente ans☐

Possédez-vous une Carte de Professionnel de Santé ?
Oui☐ Non☐

Circulation de l'information médicale

Le circuit actuel de l'information (téléphone, fax, papier) vous permet-il d'accéder à des informations exactes et fiables (intégrité) ?
Oui☐ En partie☐
Non☐ Ne sait pas☐

De même vous permet-il d'accéder à tout moment à l'information utile (disponibilité) ?
Oui☐ En partie☐
Non☐ Ne sait pas☐

Enfin, vous paraît-il de nature à garantir la confidentialité des informations médicales ?
Oui☐ En partie☐
Non☐ Ne sait pas☐

Estimez-vous que les données médicales partagées par le mode papier sont bien protégées ?

Oui☐ Non☐ Ne sait pas☐

Estimez-vous avoir de bonnes connaissances en matière de sécurité-confidentialité des informations médicales ?
Oui☐ Non☐ Ne sait pas☐

Selon vous la communication de données médicales nominatives entre professionnels de santé, en dehors d'un cadre précisé par la loi, peut-elle être sanctionnée ?
Oui☐ Non☐ Ne sait pas☐

Selon vous qui risque un préjudice (P) ou une condamnation (C) :

	Patient		Professionnel		établissement	
	P	C	P	C	P	C

En cas de communication volontaire à des tiers non autorisés ?	☐	☐	☐	☐	☐	☐
En cas d'accès par effraction	☐	☐	☐	☐	☐	☐
En cas de modification par maladresse	☐	☐	☐	☐	☐	☐
En cas d'impossibilité d'accéder aux données nécessaires (sup à 4 h)	☐	☐	☐	☐	☐	☐

Quelles peuvent être selon vous les peines encourues ?
Aucune☐ Blâme ☐
Amende☐ Prison ☐

Informatique/ sécurité

Comment évaluez-vous vos connaissances en matière de sécurité informatique des données médicales ?

Inexistantes☐ Approximatives☐ Très bonnes☐

Comme vous représentez-vous le futur système d'information informatisé (cocher trois cases) ?
Un réseau tentaculaire contrôlé par les seuls spécialistes☐
Une source de fuite d'information ☐
Une plus grande atteinte à la confidentialité des données☐
Une sophistication électronique☐
Une machine intelligente qui remplace l'homme plus efficacement ☐
Une amélioration de la coordination des soins et de la circulation de l'information☐
Un instrument de meilleure prise en charge du patient☐

Etes-vous favorable à un dossier médical informatisé partagé ?

Oui☐ Non☐ Ne sait pas☐

Doit-il être d'avantage sécurisé, entouré par des gardes-fou, que le dossier papier ?

Oui☐ Non☐ Ne sait pas☐

Quel est parmi ces deux possibilités, le risque majeur que fait courir un SI informatisé :

Le manque de confidentialité☐

L'indisponibilité, l'impossibilité d'accéder à des données☐

Autre☐ lequel

Les données médicales déjà informatisées (psydoc) vous semblent elles bien protégées ?
Oui☐ Non☐ Ne sait pas☐

Partagez-vous les informations par voie informatique en toute confiance ?

Oui☐ Non☐

Les mesures de sécurité informatique sont elles une contrainte :

Acceptable : oui ☐ non☐

Justifiée : oui ☐ non ☐

Qu'attendez-vous de l'informatisation des unités de soins ?

Une plus grande capacité d'information médicale☐

Une meilleure planification organisationnelle☐

Un meilleur accès à l'information utile en temps voulu☐

Un meilleur accès à l'information exacte, fiable ☐

Un accroissement des possibilités d'investigation médicale ☐

Une plus grande sécurité pour les soins, la prescription et l'aide au diagnostic☐

L'amélioration de la prise en charge du patient (continuité des soins, prévention) ☐

Une meilleure traçabilité de l'information☐

Souhaiteriez-vous bénéficier d'une formation à la sécurité informatique ?

Oui☐ Non☐ Ne sait pas☐

Questionnaire B (utilisateurs du SIA)

Données personnelles

Nom : (les questionnaires seront anonymés lors de l'exploitation)

Vous êtes :
Un homme☐
Une femme☐

A quel métier appartenez vous ?
Secrétaire☐ Adjoint des cadres☐ Technicien☐ Informaticien ☐
AAH☐ Direction☐ Autre☐ préciser :

Votre ancienneté dans le Centre Hospitalier Montperrin :
Est inférieure à 1 ans☐ Est supérieure à 1 ans et inférieure à 5 ans☐
Est supérieure à 5 ans et inférieure à 10 ans☐ Est supérieure à 10 ans☐

Vous avez :
Moins de trente ans☐ Plus de trente ans☐

Possédez-vous une Carte de Professionnel de Santé ?
Oui☐ Non☐

Circulation de l'information

Le circuit de l'information par la voie informatique vous permet-il d'accéder à des informations exactes et fiables (intégrité)
Oui☐ En partie☐
Non☐ Ne sait pas☐

De même vous permet-il d'accéder à tout moment à l'information utile (disponibilité) ?
Oui☐ En partie☐
Non☐ Ne sait pas☐

Enfin, vous paraît-il de nature à garantir la confidentialité des informations ?
Oui☐ En partie☐
Non☐ Ne sait pas☐

Informatique/ Sécurité

Comment évaluez-vous vos connaissances en matière de sécurité informatique ?

Inexistantes☐ Approximatives☐ Très bonnes☐

Quelle est votre représentation d'un système d'information informatisé à l'échelle de l'ensemble de l'hôpital ?
Un réseau tentaculaire contrôlé par les seuls spécialistes☐
Une source de fuite d'information ☐
Une plus grande atteinte à la confidentialité des données☐
Une sophistication électronique☐
Une machine intelligente qui remplace l'homme plus efficacement ☐
Une amélioration de la coordination des soins et de la circulation de l'information☐
Un instrument de meilleure prise en charge du patient☐

Vous arrive-t-il de communiquer votre mot de passe à un collègue?
Parfois☐ Souvent☐ Jamais☐

Ecrivez-vous votre mot de passe pour mémoire ?
Oui☐ Non☐

Avez-vous déjà oublié votre mot de passe ?
Non☐ Oui de façon marginale☐ Oui régulièrement☐

Abandonnez-vous votre poste de travail sans déconnecter votre ordinateur ?
Parfois☐ Souvent☐ Jamais☐

Ouvrez-vous un fichier attaché à un mail sans être sûr de sa provenance ?

Jamais☐ Toujours☐ Parfois☐

Partagez-vous les informations par voie informatique en toute confiance ?

Oui☐ Non☐

A quoi sont attribuables selon vous la plupart des brèches de sécurité et des dommages causés au système d'information (cocher trois cases) ?

- aux pannes matérielles et logicielles☐
- aux catastrophes naturelles☐
- à l'accès de personnes non autorisées☐
- aux interventions du personnel autorisé (erreurs)☐
- aux vols de données ou de matériel☐
- aux virus☐

Les mesures de sécurité informatique sont elles une contrainte :

Acceptable : oui ☐ non☐

Justifiée : oui ☐ non ☐

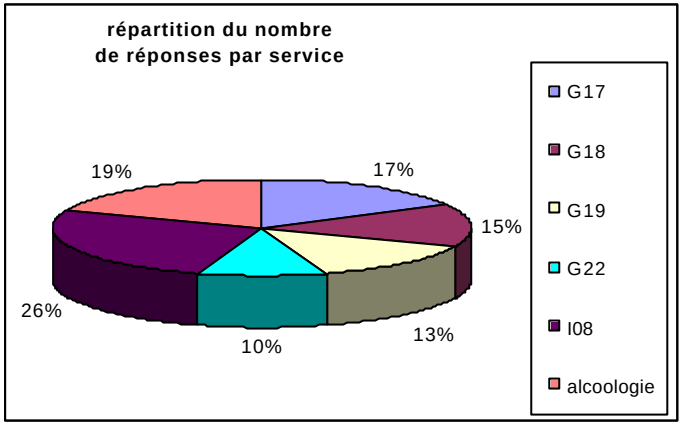
Souhaiteriez-vous bénéficier d'une formation à la sécurité du Système d'information ?

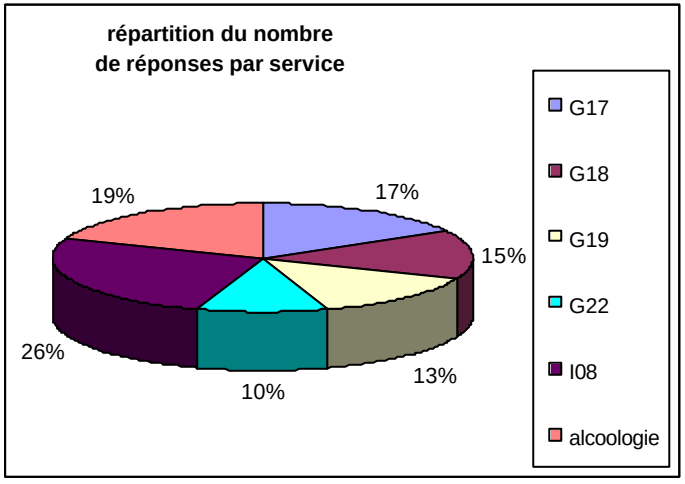
Oui☐ Non☐ Ne sait pas☐

Résultats

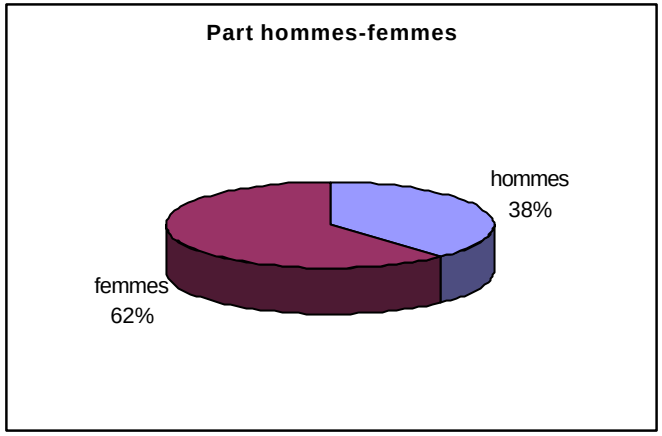
Les résultats de l'exploitation des questionnaires sont les suivants :

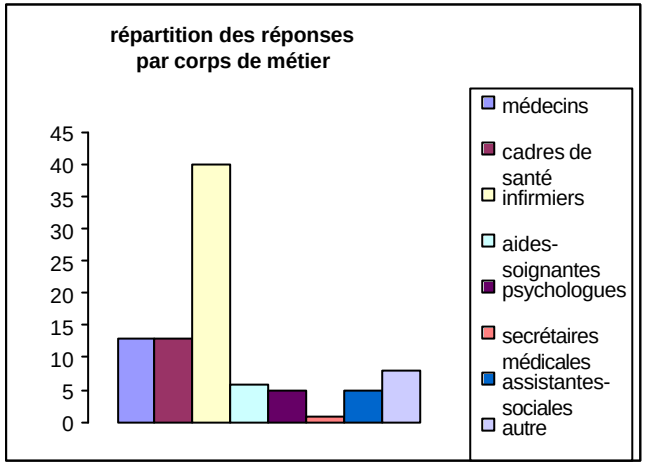
Utilisateurs du SIM

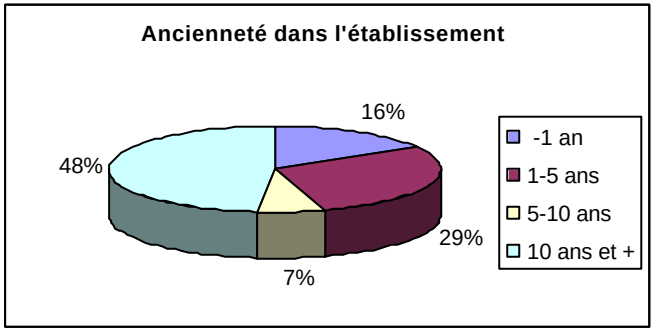


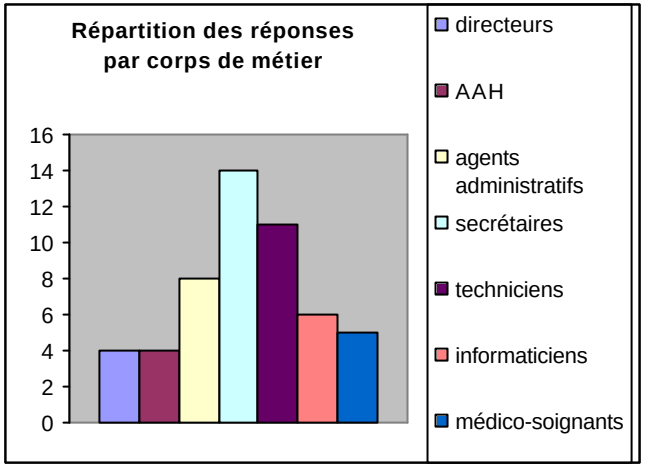


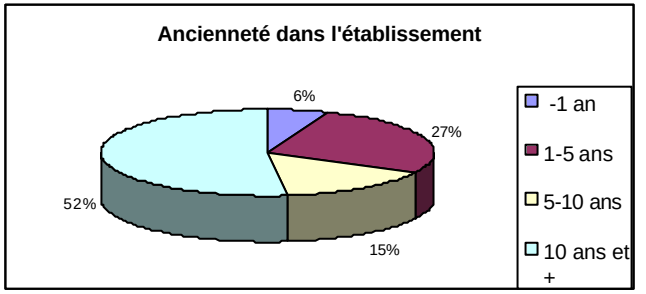
Utilisateurs du SIA



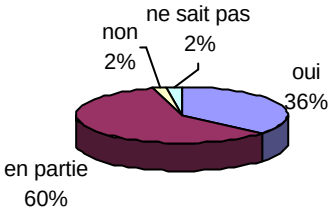

répartition des réponses
par corps de métier
45
40
35
30
25
20
15
10
5
0
médecins
cadres de santé
infirmiers
aides-soignantes
psychologues
secrétaires médicales
assistantes-sociales
autre


Ancienneté dans l'établissement
16%
48%
29%
7%
-1 an
1-5 ans
5-10 ans
10 ans et +

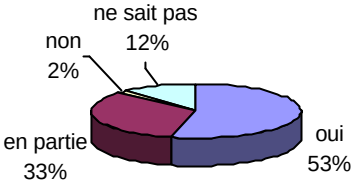

Répartition des réponses
par corps de métier
16
14
12
10
8
6
4
2
0
directeurs
AAH
agents administratifs
secrétaires
techniciens
informaticiens
médico-soignants


Ancienneté dans l'établissement
6%
27%
52%
15%
-1 an
1-5 ans
5-10 ans
10 ans et +

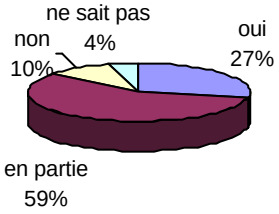
Le circuit actuel de l'information (téléphone, fax, papier) vous-permet-il d'accéder à des informations exactes et fiables (intégrité) ?



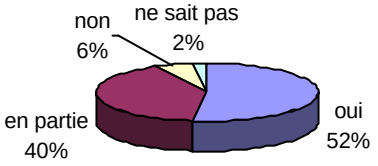
Le circuit de l'information par la voie informatique vous permet-il d'accéder à des informations exactes et fiables (intégrité) ?



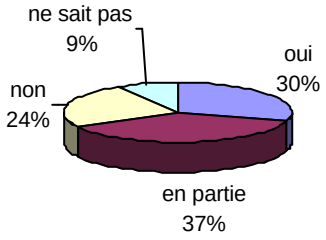
Vous permet-il d'accéder à tout moment à l'information utile ?



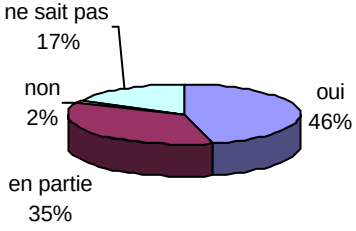
Vous permet-il d'accéder à tout moment à l'information utile (disponibilité)?



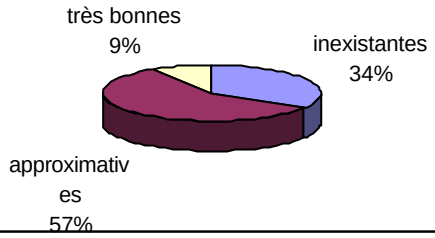
Vous paraît-il de nature à garantir la confidentialité des données médicales ?



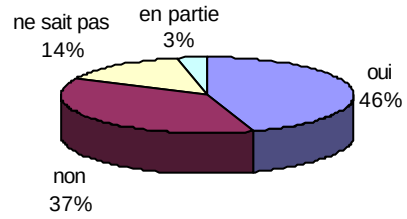
Vous paraît-il de nature à garantir la confidentialité des informations ?



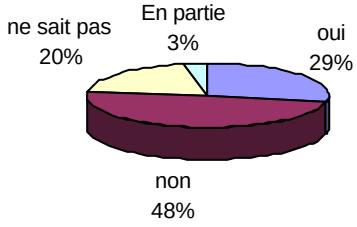
Comment évaluez-vous vos connaissances en matière de sécurité informatique des données médicales ?



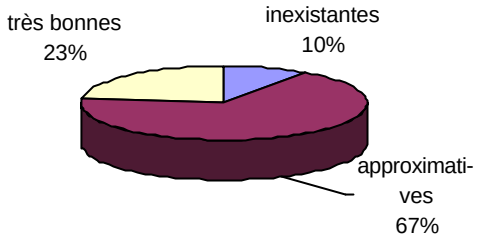
Estimez-vous avoir de bonnes connaissances en matière de sécurité-confidentialité des données médicales ?



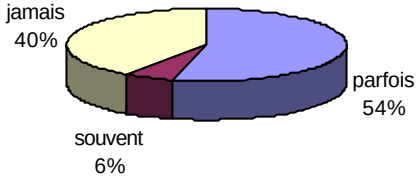
Estimez-vous que les données médicales partagées par le mode papier sont bien protégées ?



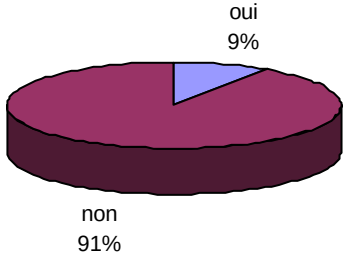
Comment évaluez-vous vos connaissances en matière de sécurité informatique ?



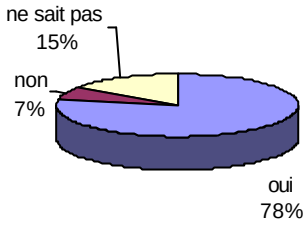
Vous arrive-t-il de communiquer votre mot de passe à un collègue ?



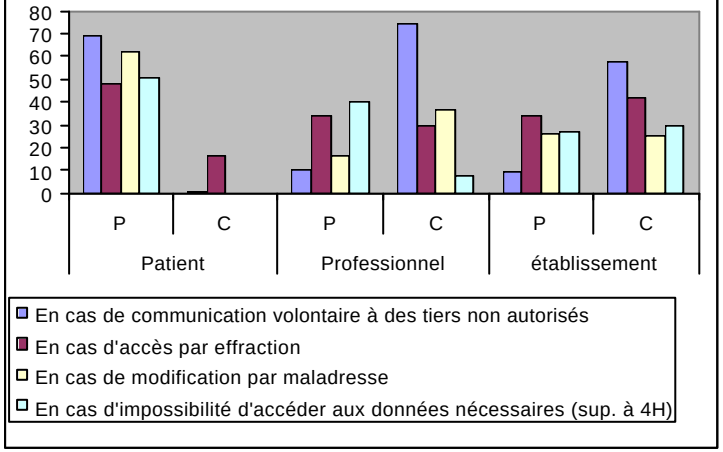
Ecrivez-vous votre mot de passe pour mémoire ?



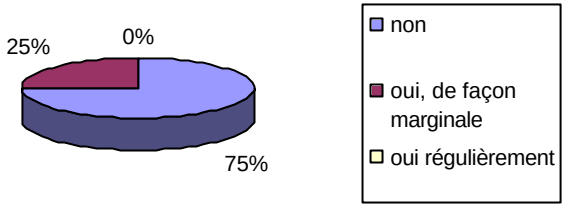
Selon vous, la communication de données médicales entre professionnels de santé, en dehors d'un cadre précisé par la loi, peut-elle être sanctionnée ?



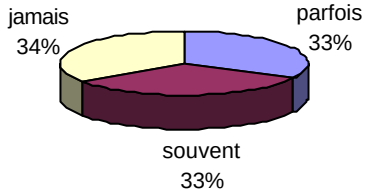
Qui risque selon vous un préjudice (P) ou une condamnation (C) ?



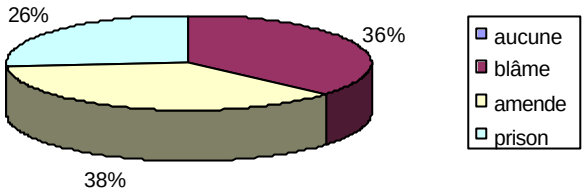
Avez-vous déjà oublié votre mot de passe ?



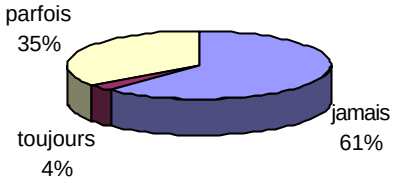
Abandonnez-vous votre poste de travail sans déconnecter votre ordinateur ?



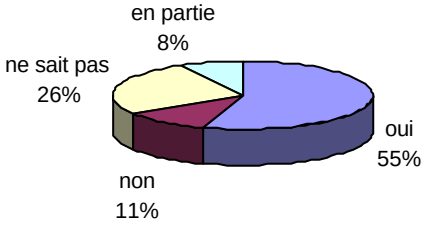
Quelles peuvent être selon vous les peines encourues ?

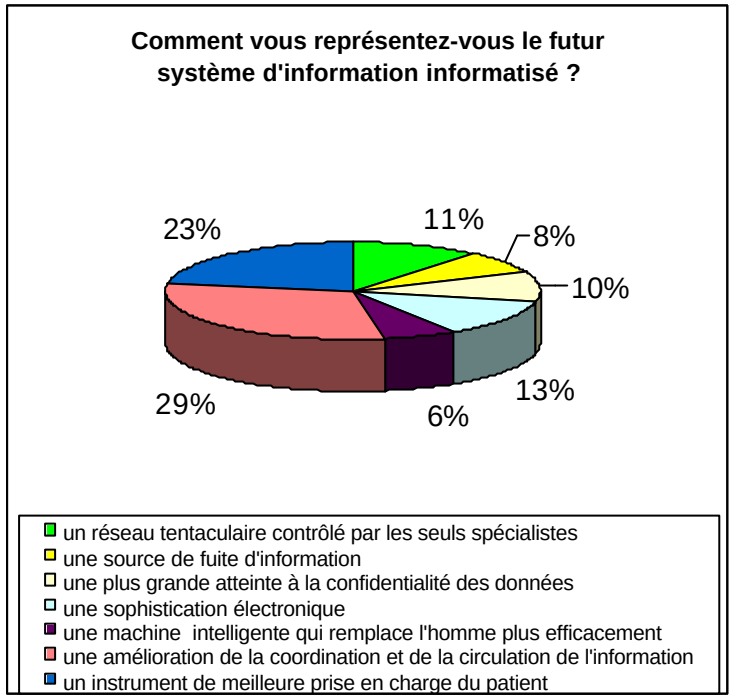


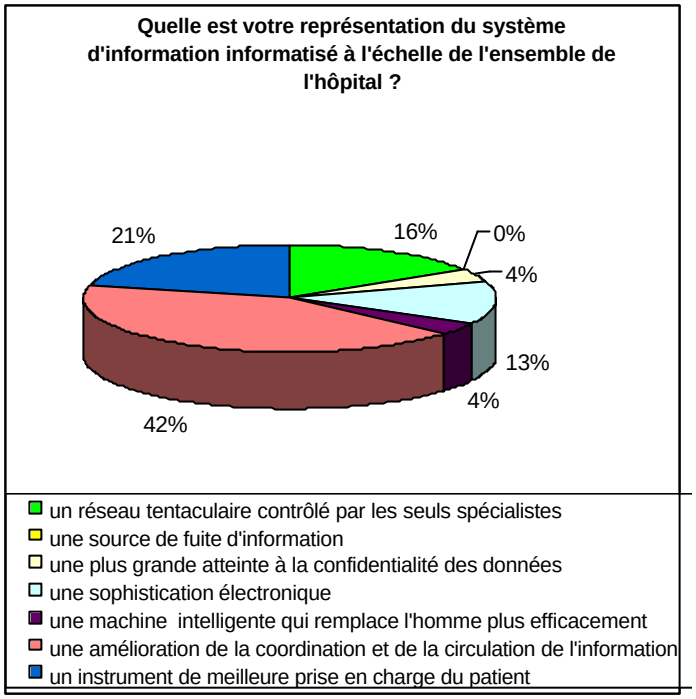
Ouvez-vous un fichier attaché à un mail sans être sûr de sa provenance ?

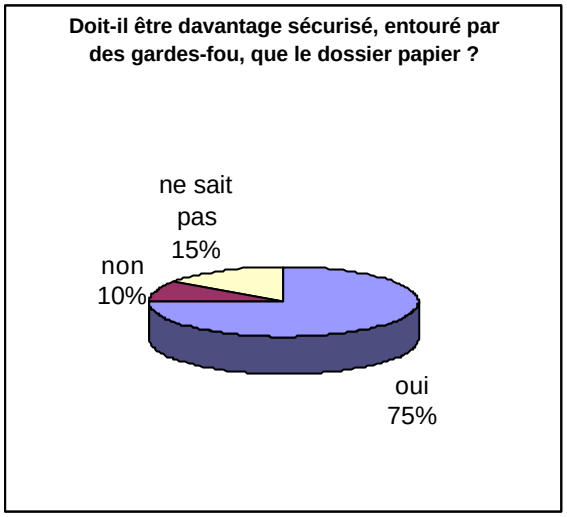


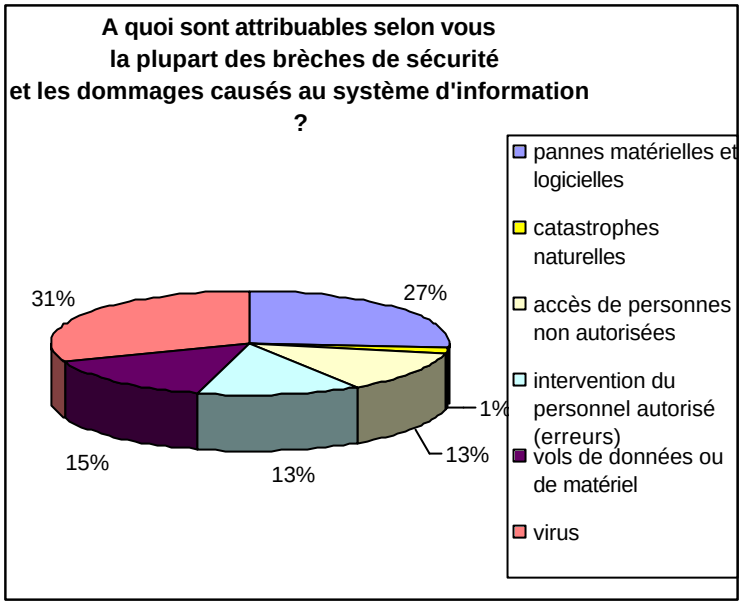
Etes-vous favorable à un dossier médical informatisé partagé ?

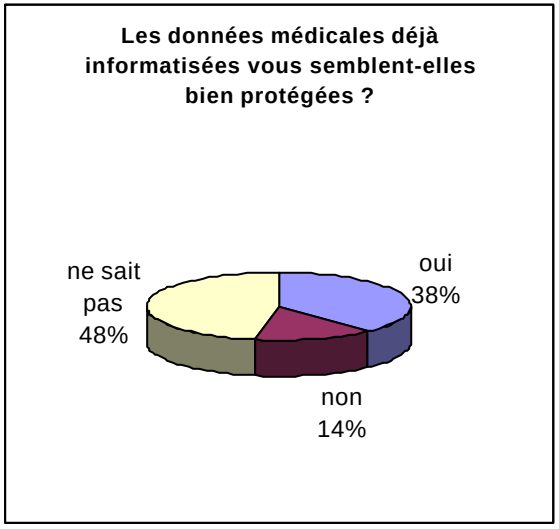


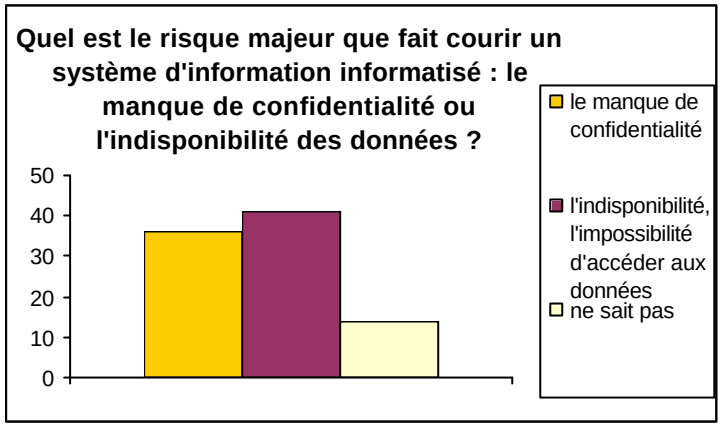

Comment vous représentez-vous le futur système d'information informatisé ?
23%
11%
8%
10%
13%
6%
29%
un réseau tentaculaire contrôlé par les seuls spécialistes
une source de fuite d'information
une plus grande atteinte à la confidentialité des données
une sophistication électronique
une machine intelligente qui remplace l'homme plus efficacement
une amélioration de la coordination et de la circulation de l'information
un instrument de meilleure prise en charge du patient

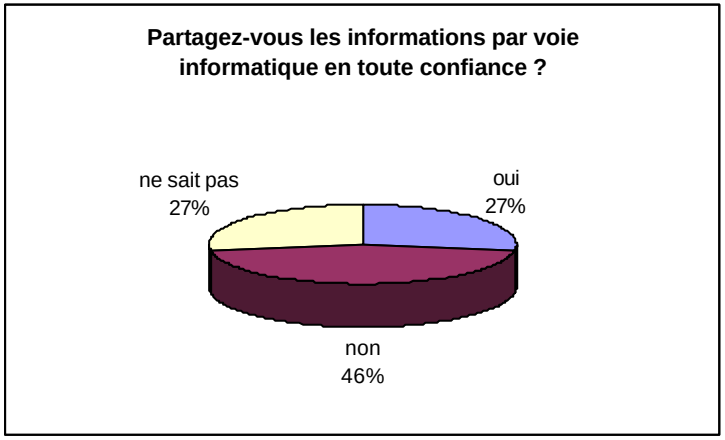

Quelle est votre représentation du système d'information informatisé à l'échelle de l'ensemble de l'hôpital ?
21%
16%
0%
4%
13%
4%
42%
un réseau tentaculaire contrôlé par les seuls spécialistes
une source de fuite d'information
une plus grande atteinte à la confidentialité des données
une sophistication électronique
une machine intelligente qui remplace l'homme plus efficacement
une amélioration de la coordination et de la circulation de l'information
un instrument de meilleure prise en charge du patient

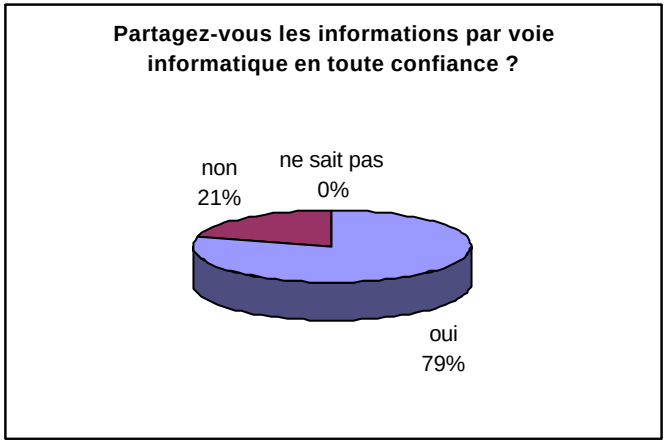

Doit-il être davantage sécurisé, entouré par des gardes-fou, que le dossier papier ?
ne sait pas 15%
non 10%
oui 75%

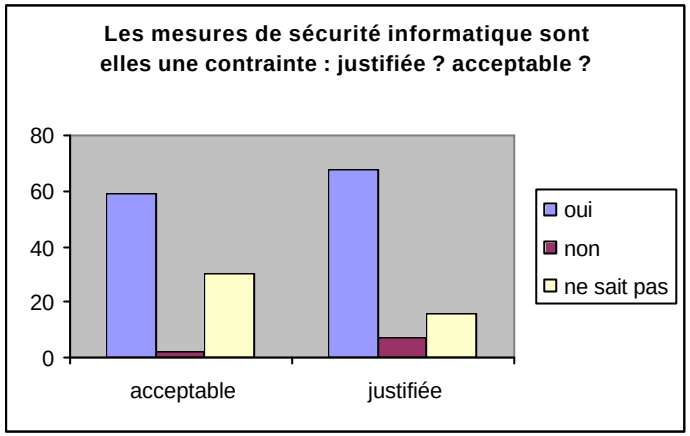

A quoi sont attribuables selon vous la plupart des brèches de sécurité et les dommages causés au système d'information ?
31%
27%
1%
13%
15%
13%
pannes matérielles et logicielles
catastrophes naturelles
accès de personnes non autorisées
intervention du personnel autorisé (erreurs)
vols de données ou de matériel
virus

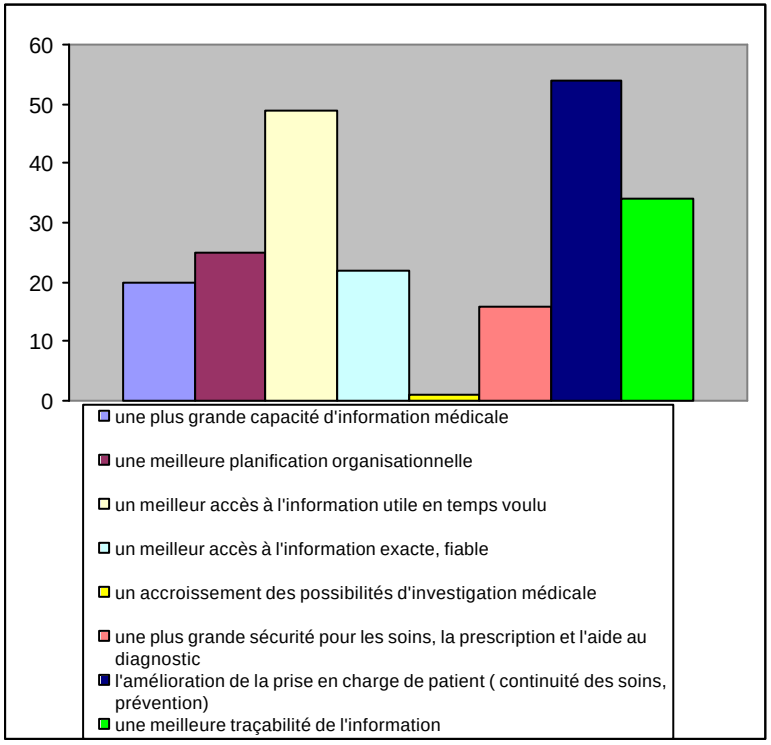

Les données médicales déjà informatisées vous semblent-elles bien protégées ?
ne sait pas 48%
oui 38%
non 14%

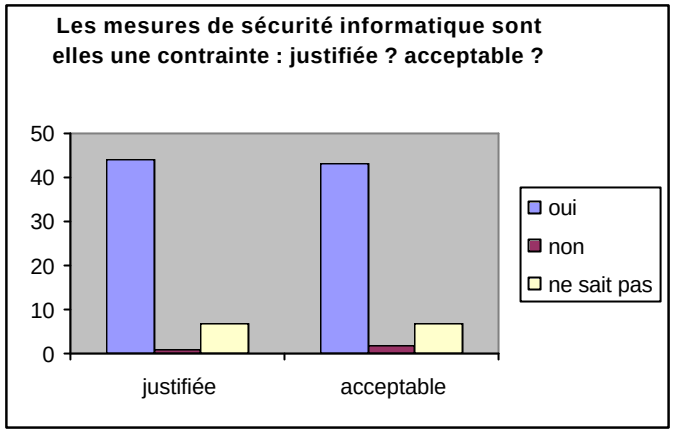

Quel est le risque majeur que fait courir un système d'information informatisé : le manque de confidentialité ou l'indisponibilité des données ?
50
40
30
20
10
0
le manque de confidentialité
l'indisponibilité, l'impossibilité d'accéder aux données
ne sait pas


Partagez-vous les informations par voie informatique en toute confiance ?
ne sait pas 27%
oui 27%
non 46%

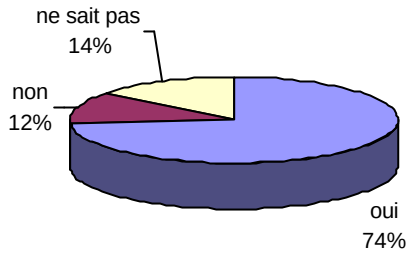

Partagez-vous les informations par voie informatique en toute confiance ?
non 21%
ne sait pas 0%
oui 79%


Les mesures de sécurité informatique sont elles une contrainte : justifiée ? acceptable ?
80
60
40
20
0
acceptable
justifiée
oui
non
ne sait pas

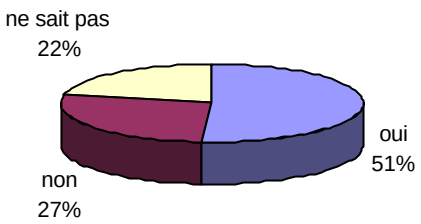

60
50
40
30
20
10
0
une plus grande capacité d'information médicale
une meilleure planification organisationnelle
un meilleur accès à l'information utile en temps voulu
un meilleur accès à l'information exacte, fiable
un accroissement des possibilités d'investigation médicale
une plus grande sécurité pour les soins, la prescription et l'aide au diagnostic
l'amélioration de la prise en charge de patient (continuité des soins, prévention)
une meilleure traçabilité de l'information


Les mesures de sécurité informatique sont elles une contrainte : justifiée ? acceptable ?
50
40
30
20
10
0
justifiée
acceptable
oui
non
ne sait pas

Souhaiteriez-vous bénéficier d'une formation à la sécurité informatique ?



Souhaiteriez-vous bénéficier d'une formation sur la sécurité informatique ?



ANNEXE II : TEXTES APPLICABLES

Extraits de la Circulaire n° 275 du 6 janvier 1989 relative à l'informatisation des hôpitaux publics

(…) Il en résulte que les hôpitaux publics sont responsables de leurs choix de matériels et de logiciels, dans le cadre des budgets hospitaliers approuvés. En effet, les applications informatiques doivent être adaptées à l'activité de chaque hôpital, traduite dans son projet d'établissement Elles doivent servir sa politique d'établissement dans une perspective de maîtrise des coûts, l'investissement informatique devant être un investissement de productivité.

(…)

I. - Un schéma directeur informatique au service du système d'information de l'hôpital

Le système d'information de l'hôpital peut être défini comme l'ensemble des informations, de leurs règles de circulation et de traitement nécessaires à son fonctionnement quotidien, à ses modes de gestion et d'évaluation ainsi qu'à son processus de décision stratégique.

A. - La priorité: le système d'information de l'hôpital

Il importe que chaque hôpital, en fonction de sa stratégie et de ses objectifs analyse et adapte son système d'information, en concertation avec les différents acteurs concernes, de manière à assurer la cohérence entre les soins donnés aux malades et la gestion de l'établissement.

Ainsi, il appartient à chaque établissement de mettre en place un tronc commun minimum d'informations administratives et médicales permettant aux différents acteurs du service public hospitalier d'obtenir un ensemble d'informations fiables et cohérentes, nécessaires à l'analyse de l'activité des établissements et à la mise en place des indicateurs utiles à la gestion. Ces informations pourront être synthétisées à partir des données fournies par les services. Les informations qui ne sont pas utiles au sous-ensemble commun d'informations médicales et administratives constituent le système propre à chaque service.

Ce système d'information médico-administratif doit être soumis aux organes de gestion des établissements.

B. - Le cadre réglementaire et institutionnel

L'outil informatique doit être conçu de manière à permettre aux établissements de répondre à l'évolution de la réglementation édictée par l'État, et aux dispositions de la loi du 6 janvier 1978 dite << Informatique et libertés >>.

A ce titre, les applications informatiques novatrices relatives au domaine médical et l'utilisation de technologies nouvelles dans le domaine informatique impliquant les acteurs de santé doivent être conformes à la déontologie médicale.

C. - Le schéma directeur

A partir de l'analyse de son système d'information, l'établissement définit globalement ses besoins d'informatisation et établit un programme pluriannuel à moyen terme, périodiquement actualisé, de sa mise en oeuvre.

Ces éléments sont consignés dans un schéma directeur qui en présente les aspects organisationnels, techniques, économiques et financiers, document de référence assurant la cohérence et la continuité de l'exécution des différentes phases de cette informatisation. Sa mise en oeuvre est spécifie dans les plans d'actions annuels.

Les choix informatiques des hôpitaux, s'ils relèvent de leur entière responsabilité doivent s'inscrire dans le cadre réglementaire fixe en matière budgétaire et financière.

Ainsi, sur le plan financier, la réalisation d'un schéma directeur informatique - qui se traduit notamment par des opérations d'investissement - doit être appréhendée de la même façon que les autres opérations d'investissement, et dans le respect des règles fixées pour ces dernières. Les dépenses afférentes à l'informatique, tant de fonctionnement que d'investissement, doivent donc être examinées dans une perspective pluriannuelle.

Les conséquences budgétaires, et notamment les surcoûts de fonctionnement, devront faire l'objet d'une compensation intégrale sur le budget propre de l'établissement ou au-delà des moyens de l'établissement dans le cadre strict de l'enveloppe départementale, à l'instar des autres opérations d'investissement.

Des économies nettes doivent être recherchées, les opérations d'informatisation étant avant tout des opérations productives. La survenance de surcoûts ne doit être que temporaire avant de laisser place les années ultérieures à des gains de productivité.

Il est rappelé enfin que le financement des investissements liés au traitement de l'information peut être effectue par recours au crédit-bail, conformément aux dispositions réglementaires.

II. - L'action des pouvoirs publics

Cette action s'applique à trois domaines:

A. - La normalisation d'informations obligatoires

Un certain nombre d'informations, véhiculées et traitées par les systèmes informatiques des hôpitaux, sont soumises à une réglementation nationale relevant du ministère de la solidarité, de la santé et de la protection sociale, du ministère de l'économie et des finances ou d'autres départements ministériels.

Les domaines concernés par cette normalisation sont les suivants:

paie des agents;

informations relatives au bilan social;

facturation des prestations des hôpitaux;

prises en charge, états de séjour et dotation globale:

comptabilité générale et analytique des établissements, et présentation budgétaire;

informations statistiques dans le cadre des enquêtes nationales ou régionales prévues réglementairement;

conséquences des applications << Agir >> et << Tutelle >> dans les relations avec les autorités de tutelle;

P.M.S.I. (production de R.S.S. et de G.H.M.).

La réglementation précisera leur nature, leur format et leurs modalités de transmission, que les systèmes informatiques des hôpitaux respecteront, aussi bien dans la production de ces informations que dans leur transmission à leurs partenaires.

B. - L'aide à l'élaboration de logiciels

L'action du ministère sera orientée vers:

l'aide à la mise au point de solutions informatiques économiques, en particulier par la réalisation de cahiers des charges;

la concertation entre l'administration centrale et les partenaires hospitaliers concernes qui portera notamment sur la résolution de problèmes juridiques.

C. - Normalisation technique

L'ouverture des systèmes informatiques à l'intégration de matériels et de logiciels hétérogènes devant communiquer impose le suivi des normes définies par les organismes nationaux et internationaux: I.S.O./C.E.I., C.C.I.T.T., C.E.P.T., C.E.N./CENELEC, AFNOR

Les schémas directeurs feront explicitement référence aux normes utilisées.

D. - Contrôle

Les normes et les standards imposes pour les logiciels d'application de la réglementation seront transmis à toutes les instances susceptibles d'effectuer des contrôles sur les établissements publics hospitaliers. En particulier, les actions de contrôle de l'inspection générale des affaires sociales pourront porter, à la demande du ministre, sur le respect de ces normes par les systèmes informatiques hospitaliers.

III. - Les actions à entreprendre

Le développement de l'informatique décentralisée et repartie dans les hôpitaux suppose que ce changement soit maîtrise par les hospitaliers eux-mêmes.

Des actions seront menées dans les domaines suivants :

A. - Les actions de formation

Les établissements hospitaliers doivent à la fois conserver la maîtrise de l'outil technique et mettre en place des solutions répondant aux besoins exacts des utilisateurs.

La formation des utilisateurs préalable à l'analyse du système d'information hospitalier et au dialogue avec les informaticiens est à cet égard un élément déterminant. Des actions de formation pluridisciplinaire permettront d'établir une analyse commune aux

personnels paramédicaux, médicaux et administratifs afin de dégager les priorités de l'établissement en matière de schéma directeur.

Ces actions de formation concernent aussi les techniciens de l'informatique. Des comparaisons avec les niveaux de formation du secteur privé devraient permettre d'apprécier les efforts à engager afin de conserver à un bon niveau et, le cas échéant, d'adapter à des métiers qui ont profondément évolue les pratiques des informaticiens hospitaliers.

B. - La gestion du système d'information et de ses implications informatiques par les hospitaliers

** Le responsable du système d'information et d'organisation.*

Dans la mesure où le lui permettent sa taille et ses moyens humains, il est important que l'hôpital se dote de personnel qualifié, responsable de la gestion de l'information. Ainsi il parait nécessaire de poursuivre le développement des fonctions de gestion du système d'information et d'organisation dans les hôpitaux. Ces fonctions selon les possibilités de l'établissement et à titre indicatif, pourront être prises en charge par:

un cadre de direction a temps plein dans les centres hospitaliers de plus de 1 000 lits

un cadre de direction à temps plein ou à temps partiel dans les centres hospitaliers de 500 à 1000 lits:

un cadre administratif à temps plein ou à temps partiel dans les établissements de moins de 500 lits.

En effet, le responsable du système d'information et d'organisation (R.S.I.O.) est le garant du bon fonctionnement du système d'information et de sa pertinence pour:

contribuer à la qualité du service;

permettre une gestion performante de l'établissement:

fournir les informations demandées par la réglementation:

faciliter les prises de décision concernant les choix d'évolution d'activité de niveau stratégique.

Selon la taille et l'organisation de l'établissement, il coordonne ou est le responsable hiérarchique direct des cellules d'analyse de gestion, d'organisation et d'information.

De façon continue le R.S.I.O. doit gérer le système d'information c'est-à-dire vérifier que chaque centre de responsabilité dispose bien des informations qui lui sont nécessaires et que ces informations sont fiables. Il est responsable de la production des informations nécessaires à la direction et de celles demandées par la réglementation.

Il doit assurer 1a cohérence du système d'information et veiller à l'articulation entre les systèmes d'information administratifs et les systèmes de gestion de l'information médicale.

Le R.S.I.O. a pour tâche d'analyser le système d'information existant, d'étudier sa cohérence avec l'organisation socio-technique en place, le fonctionnement de la structure et les objectifs à atteindre.

Il doit être à même de proposer des modifications et de planifier dans un schéma directeur, la mise en place de procédures et d'outils de stockage, de traitement et de circulation de l'information permettant d'atteindre les objectifs de la direction. Pour cela, il doit pouvoir conseiller les utilisateurs, y compris en termes d'organisation, et définir avec eux les flux d'information, les moyens à mettre en place et la rentabilité d'un système.

Étant donne qu'il doit avoir une vue globale de l'établissement et un rôle de coordination et de conseil auprès des différents services il est souhaitable que le R.S.I.O. soit un cadre administratif rattaché au directeur.

Le R.S.I.O. a un profil de généraliste ayant des connaissances en matière de sociologie des organisations, de systèmes d'information de gestion d'un établissement

** La gestion de l'information médicale.*

L'information médicale décrit l'état de santé des malades et les actes et protocoles thérapeutiques qu'ils doivent subir. L'informatique médicale effectue des traitements afférents à cette information. Une structure de gestion de l'information médicale sera constituée à l'initiative des établissements. Elle prendra la forme d'un département de l'information médicale dans les établissements disposant d'au moins 200 lits de court séjour.

Gérer l'information médicale c'est, en liaison avec le R.S.I.O. contribuer à la cohérence globale des fonctions du système d'information hospitalier à tous les stades de la prise en charge du patient par les unités de soins et les unités medico-techniques: ces fonctions s'articulent autour de trois pôles prioritaires: le dossier du patient, la planification des soins, la communication interne et externe à l'établissement.

La structure de gestion de l'information médicale supervise le fonctionnement du système d'information générateur du dossier minimum commun du patient d'où seront extraits les éléments nécessaires au suivi de l'activité des services: elle s'assure de la qualité des données (exhaustivité de la collecte, harmonisation du codage, vraisemblance des données), elle participe à la mise en forme des modalités de présentation des informations elle explicite les différentes étapes d'agrégation que subissent les données (modalités de chaînage de séjours, logique de classification, etc.): son fonctionnement est supervisé par une commission des pairs, émanation de la C.M.E..

C. - La liberté de choix des établissements et la coopération interhospitalière

Les établissements peuvent s'adresser aux fournisseurs de leur choix, dans le respect du code des marches publics.

Les structures régionales (C.R.I.H., S.I.R.) ont constitué un élément moteur du développement de l'informatique hospitalière et devraient continuer à s'inscrire comme une composante importante de l'offre sur ce marché. Les hôpitaux pourront décider de continuer

ou non d'adhérer au C.R.I.H. auxquels ils sont liés actuellement, ou d'adhérer ou non à un autre C.R.I.H. et de bénéficier de certaines des prestations par voie de convention.

La liberté de choix des hôpitaux doit permettre de stimuler le marché de l'informatique hospitalière et de proposer des solutions concurrentielles répondant aux multiples besoins des hôpitaux.

Cependant l'importance des moyens humains, matériels et financiers nécessaires à l'élaboration d'une informatique de qualité montre que la coopération interhospitaliere, ainsi que la mise en commun de moyens humains et financiers ont permis la réalisation de solutions inabordables pour un seul établissement, ainsi qu'une incitation décisive à l'investissement des sociétés privées ou des C.R.I.

Extraits de la Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie

(…) I. - Après l'article L. 161-36 du code de la sécurité sociale, il est inséré un article L. 161-36-1 A ainsi rédigé :

« Art. L. 161-36-1 A. - I. - Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant.

« Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé ainsi qu'à tous les professionnels intervenant dans le système de santé.

« Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible. Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe.

« Afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique, comme leur transmission par voie électronique entre professionnels, sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des

libertés. Ce décret détermine les cas où l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 est obligatoire.

« Le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 EUR d'amende.

« En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance définie à l'article L. 1111-6 du code de la santé publique reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celle-ci, sauf opposition de sa part. Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations.

« Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès. »

II. - Le sixième alinéa de l'article L. 1110-4 du code de la santé publique est complété par une phrase ainsi rédigée : « Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations. »

Article 3

I. - Le chapitre Ier du titre VI du livre Ier du code de la sécurité sociale est complété par une section 5 ainsi rédigée :

« Section 5 « Dossier médical personnel

« Art. L. 161-36-1. - Afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé, chaque bénéficiaire de l'assurance maladie dispose, dans les conditions et sous les garanties prévues à l'article L. 1111-8 du code de la santé publique et dans le respect du secret médical, d'un dossier médical personnel constitué de l'ensemble des données mentionnées à l'article L. 1111-8 du même code, notamment des informations qui permettent le suivi des actes et prestations de soins. Le dossier médical personnel comporte également un volet spécialement destiné à la prévention.

« Ce dossier médical personnel est créé auprès d'un hébergeur de données de santé à caractère personnel agréé dans les conditions prévues à l'article L. 1111-8 du même code.

« L'adhésion aux conventions nationales régissant les rapports entre les organismes d'assurance maladie et les professionnels de santé, prévues à l'article L. 162-5 du présent code, et son maintien sont subordonnés à la consultation ou à la mise à jour du dossier médical personnel de la personne prise en charge par le médecin.

« Les dispositions de l'alinéa précédent sont applicables à compter du 1er janvier 2007.

« Art. L. 161-36-2. - Dans le respect des règles déontologiques qui lui sont applicables ainsi que des dispositions des articles L. 1110-4 et L. 1111-2 du code de la santé publique, et selon les modalités prévues à l'article L. 1111-8 du même code, chaque professionnel de

santé, exerçant en ville ou en établissement de santé, quel que soit son mode d'exercice, reporte dans le dossier médical personnel, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge. En outre, à l'occasion du séjour d'un patient, les professionnels de santé habilités des établissements de santé reportent sur le dossier médical personnel les principaux éléments résumés relatifs à ce séjour.

« Le niveau de prise en charge des actes et prestations de soins par l'assurance maladie prévu à l'article L. 322-2 est subordonné à l'autorisation que donne le patient, à chaque consultation ou hospitalisation, aux professionnels de santé auxquels il a recours, d'accéder à son dossier médical personnel et de le compléter. Le professionnel de santé est tenu d'indiquer, lors de l'établissement des documents nécessaires au remboursement ou à la prise en charge, s'il a été en mesure d'accéder au dossier.

« Les dispositions de l'alinéa précédent ne s'appliquent pas aux personnes visées aux chapitres Ier à V du titre VI du livre VII pour les soins reçus à l'étranger ou à l'occasion d'un séjour temporaire en France.

« Art. L. 161-36-3. - L'accès au dossier médical personnel ne peut être exigé en dehors des cas prévus à l'article L. 161-36-2, même avec l'accord de la personne concernée.

« L'accès au dossier médical personnel est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application.

« Le dossier médical personnel n'est pas accessible dans le cadre de la médecine du travail.

« Tout manquement aux présentes dispositions donne lieu à l'application des peines prévues à l'article 226-13 du code pénal.

Extraits de la Loi n°83-634 du 17 juillet 1983, portant droits et obligations des fonctionnaires

Article 26 : Les fonctionnaires sont tenus au secret professionnel dans le cadre des règles instituées dans le code pénal.

Les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions.

En dehors des cas expressément prévus par la réglementation en vigueur, notamment en matière de liberté d'accès aux documents administratifs, les fonctionnaires ne peuvent être

déliés de cette obligation de discrétion professionnelle que par décision expresse de l'autorité dont ils dépendent.

Article 29 : Toute faute commise par un fonctionnaire dans l'exercice ou à l'occasion de l'exercice de ses fonctions l'expose à une sanction disciplinaire sans préjudice, le cas échéant, des peines prévues par la loi pénale.

Extraits de la Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Article 1 : Les articles 2 à 5 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés sont ainsi rédigés :

« Art. 2. - La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

« Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

« La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.

« Art. 3. - I. - Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce

traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

« II. - Le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires.

(…)

« II. - Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui. »

Article 2 : Le chapitre II de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« Chapitre II : « Conditions de licéité des traitements de données à caractère personnel

« Section 1 : Dispositions générales

« Art. 6. - Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

« 1° Les données sont collectées et traitées de manière loyale et licite ;

« 2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

« 3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

« 4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

« 5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

« Art. 7. - Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :

« 1° Le respect d'une obligation légale incombant au responsable du traitement ;

« 2° La sauvegarde de la vie de la personne concernée ;
« 3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
« 4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
« 5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.
« Section 2 : Dispositions propres à certaines catégories de données
« Art. 8. - I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.
« II. - Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :
« 1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ;
« 2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;
« 3° Les traitements mis en oeuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :
« - pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ;
« - sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;
« - et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;
« 4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;
« 5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
« 6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en oeuvre par un membre d'une profession de santé, ou par une autre personne

à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;

« 7° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ;

« 8° Les traitements nécessaires à la recherche dans le domaine de la santé selon les modalités prévues au chapitre IX.

« III. - Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions des chapitres IX et X ne sont pas applicables.

« IV. - De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26.

« Art. 9. - Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en oeuvre que par :

« 1° Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;

« 2° Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ;

« 3° [Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel n° 2004-499 DC du 29 juillet 2004 ;]

« 4° Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres Ier, II et III du même code aux fins d'assurer la défense de ces droits.

« Art. 10. - Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

« Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

« Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour

lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée. »

(…)

Chapitre IV de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« Chapitre IV : Formalités préalables à la mise en oeuvre des traitements

« Art. 22. - I. - A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés.

« II. - Toutefois, ne sont soumis à aucune des formalités préalables prévues au présent chapitre :

« 1° Les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

« 2° Les traitements mentionnés au 3° du II de l'article 8.

« III. - Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé.

« La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel.

« Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions.

« En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés.

« IV. - Le responsable d'un traitement de données à caractère personnel qui n'est soumis à aucune des formalités prévues au présent chapitre communique à toute personne qui en fait la demande les informations relatives à ce traitement mentionnées aux 2° à 6° du I de l'article 31.

« Section 1 : « Déclaration

« Art. 23. - I. - La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

« Elle peut être adressée à la Commission nationale de l'informatique et des libertés par voie électronique.

« La commission délivre sans délai un récépissé, le cas échéant par voie électronique. Le demandeur peut mettre en oeuvre le traitement dès réception de ce récépissé ; il n'est exonéré d'aucune de ses responsabilités.

« II. - Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Dans ce cas, les informations requises en application de l'article 30 ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

« Art. 24. - I. - Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en oeuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit et publie, après avoir reçu le cas échéant les propositions formulées par les représentants des organismes publics et privés représentatifs, des normes destinées à simplifier l'obligation de déclaration.

« Ces normes précisent :

« 1° Les finalités des traitements faisant l'objet d'une déclaration simplifiée ;

« 2° Les données à caractère personnel ou catégories de données à caractère personnel traitées ;

« 3° La ou les catégories de personnes concernées ;

« 4° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel sont communiquées ;

« 5° La durée de conservation des données à caractère personnel.

« Les traitements qui correspondent à l'une de ces normes font l'objet d'une déclaration simplifiée de conformité envoyée à la commission, le cas échéant par voie électronique.

« II. - La commission peut définir, parmi les catégories de traitements mentionnés au I, celles qui, compte tenu de leurs finalités, de leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées, sont dispensées de déclaration.

« Dans les mêmes conditions, la commission peut autoriser les responsables de certaines catégories de traitements à procéder à une déclaration unique selon les dispositions du II de l'article 23.

« Section 2 : Autorisation

« Art. 25. - I. - Sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :

« 1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ;

« 2° Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en oeuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ;

« 3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en oeuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;

« 4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;

(…)

Article 5

Le chapitre V de la loi n° 78-17 du 6 janvier 1978 précitée est intitulé : « Obligations incombant aux responsables de traitements et droits des personnes ». Ce chapitre comprend les articles 32 à 42 ainsi que l'article 40, qui devient l'article 43. Il comprend deux sections ainsi rédigées :

« Section 1 : Obligations incombant aux responsables de traitements

« Art. 32. - I. - La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

« 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;

« 2° De la finalité poursuivie par le traitement auquel les données sont destinées ;

« 3° Du caractère obligatoire ou facultatif des réponses ;

« 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;

« 5° Des destinataires ou catégories de destinataires des données ;

« 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ;

« 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.

« Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°.

« II. - Toute personne utilisatrice des réseaux de communications électroniques doit être informée de manière claire et complète par le responsable du traitement ou son représentant

« - de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;

« - des moyens dont elle dispose pour s'y opposer.

« Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

« - soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

« - soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

« III. - Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.

« Lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas aux traitements nécessaires à la conservation de ces données à des fins historiques, statistiques ou scientifiques, dans les conditions prévues au livre II du code du patrimoine ou à la réutilisation de ces données à des fins statistiques dans les conditions de l'article 7 bis de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

« IV. - Si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à celles mentionnées au 1° et au 2° du I.

(…)

« Art. 34. - Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

« Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8.

« Art. 35. - Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

« Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.

« Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en oeuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

« Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

« Art. 36. - Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-4 du code du patrimoine.

« Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives dans le cadre du livre II du même code sont dispensés des formalités préalables à la mise en oeuvre des traitements prévues au chapitre IV de la présente loi.

« Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées au premier alinéa :

« - soit avec l'accord exprès de la personne concernée ;

« - soit avec l'autorisation de la Commission nationale de l'informatique et des libertés ;

« - soit dans les conditions prévues au 8° du II et au IV de l'article 8 s'agissant de données mentionnées au I de ce même article.

« Art. 37. - Les dispositions de la présente loi ne font pas obstacle à l'application, au bénéfice de tiers, des dispositions du titre Ier de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal et des dispositions du livre II du code du patrimoine.

« En conséquence, ne peut être regardé comme un tiers non autorisé au sens de l'article 34 le titulaire d'un droit d'accès aux documents administratifs ou aux archives publiques exercé conformément à la loi n° 78-753 du 17 juillet 1978 précitée et au livre II du même code.

« Section 2 : Droits des personnes à l'égard des traitements de données à caractère personnel

« Art. 38. - Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

« Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.

« Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement.

« Art. 39. - I. - Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :

« 1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

« 2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

« 3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne

« 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

« 5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle.

« Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

« En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition.

« II. - Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées.

« Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la Commission nationale de l'informatique et des libertés.

« Art. 40. - Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

« Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

« En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.

« Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39.

« Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.

« Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

« Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

(…)

Article 6 : Le chapitre VI de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« Chapitre VI : « Le contrôle de la mise en oeuvre des traitements

« Art. 44. - I. - Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en oeuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

« Le procureur de la République territorialement compétent en est préalablement informé.

« II. - En cas d'opposition du responsable des lieux, la visite ne peut se dérouler qu'avec l'autorisation du président du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter ou du juge délégué par lui.

« Ce magistrat est saisi à la requête du président de la commission. Il statue par une ordonnance motivée, conformément aux dispositions prévues aux articles 493 à 498 du nouveau code de procédure civile. La procédure est sans représentation obligatoire.

« La visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée. Celui-ci peut se rendre dans les locaux durant l'intervention. A tout moment, il peut décider l'arrêt ou la suspension de la visite.

« III. - Les membres de la commission et les agents mentionnés au premier alinéa du I peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie ; ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles ; ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

« Ils peuvent, à la demande du président de la commission, être assistés par des experts désignés par l'autorité dont ceux-ci dépendent.

« Seul un médecin peut requérir la communication de données médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion de service de santé, et qui est mis en oeuvre par un membre d'une profession de santé.

« Il est dressé contradictoirement procès-verbal des vérifications et visites menées en application du présent article.

« IV. - Pour les traitements intéressant la sûreté de l'Etat et qui sont dispensés de la publication de l'acte réglementaire qui les autorise en application du III de l'article 26, le décret en Conseil d'Etat qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis aux dispositions du présent article. »

Article 7

Le chapitre VII de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« Chapitre VII : « Sanctions prononcées par la Commission nationale de l'informatique et des libertés

« Art. 45. - I. - La Commission nationale de l'informatique et des libertés peut prononcer un avertissement à l'égard du responsable d'un traitement qui ne respecte pas les obligations découlant de la présente loi. Elle peut également mettre en demeure ce responsable de faire cesser le manquement constaté dans un délai qu'elle fixe.

« Si le responsable d'un traitement ne se conforme pas à la mise en demeure qui lui est adressée, la commission peut prononcer à son encontre, après une procédure contradictoire, les sanctions suivantes :

« 1° Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en oeuvre par l'Etat ;

« 2° Une injonction de cesser le traitement, lorsque celui-ci relève des dispositions de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.

« II. - En cas d'urgence, lorsque la mise en oeuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la commission peut, après une procédure contradictoire :

« 1° Décider l'interruption de la mise en oeuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26, ou de ceux mentionnés à l'article 27 mis en oeuvre par l'Etat ;

« 2° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ;

« 3° Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ; le Premier ministre fait alors connaître à la commission les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

« III. - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.

« Art. 46. - Les sanctions prévues au I et au 1° du II de l'article 45 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable du traitement, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la commission mais ne prend pas part à ses délibérations. La commission peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information.

« La commission peut rendre publics les avertissements qu'elle prononce. Elle peut également, en cas de mauvaise foi du responsable du traitement, ordonner l'insertion des autres sanctions qu'elle prononce dans des publications, journaux et supports qu'elle désigne. Les frais sont supportés par les personnes sanctionnées.

« Les décisions prises par la commission au titre de l'article 45 sont motivées et notifiées au responsable du traitement. Les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat.

« Art. 47. - Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.

« Lors du premier manquement, il ne peut excéder 150 000 EUR. En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 300 000 EUR ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 EUR.

« Lorsque la Commission nationale de l'informatique et des libertés a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.

« Les sanctions pécuniaires sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.

« Art. 48. - La commission peut exercer les pouvoirs prévus à l'article 44 ainsi qu'au I, au 1° du II et au III de l'article 45 à l'égard des traitements dont les opérations sont mises en oeuvre, en tout ou partie, sur le territoire national, y compris lorsque le responsable du traitement est établi sur le territoire d'un autre Etat membre de la Communauté européenne.

« Art. 49. - La commission peut, à la demande d'une autorité exerçant des compétences analogues aux siennes dans un autre Etat membre de la Communauté européenne, procéder à des vérifications dans les mêmes conditions, selon les mêmes procédures et sous les mêmes sanctions que celles prévues à l'article 45, sauf s'il s'agit d'un traitement mentionné au I ou au II de l'article 26.

« La commission est habilitée à communiquer les informations qu'elle recueille ou qu'elle détient, à leur demande, aux autorités exerçant des compétences analogues aux siennes dans d'autres Etats membres de la Communauté européenne. »

Article 8 : La loi n° 78-17 du 6 janvier 1978 précitée est complétée par un chapitre VIII ainsi rédigé :

« Chapitre VIII : Dispositions pénales

« Art. 50. - Les infractions aux dispositions de la présente loi sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

« Art. 51. - Est puni d'un an d'emprisonnement et de 15 000 EUR d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés :

« 1° Soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 ;

« 2° Soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;

« 3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.

(…)

6° Le premier alinéa de l'article 40-4 est ainsi rédigé :

« Toute personne a le droit de s'opposer à ce que les données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux qui sont visés à l'article 53. » ;

(…)

Dispositions du Code pénal s'appliquant aux infractions des dispositions prévues par la Loi n°78-17 du 6 janvier 1978 modifiée par la loi 2004-801 du 6 août 2004

Secret professionnel

Article 226-13 : La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende.

Protection juridique des personnes

Le non-respect de la vie privée et les atteintes à la personnalité de l'individu par la constitution ou l'exploitation de fichiers ou de traitements automatisés sont sanctionnés par les articles ci-dessous reproduits du Code pénal.

Art. 226-16. - Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende.

« Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Art. 226-16-1 A - Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende.

Art. 226-16-1. - Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il

porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende.

Art. 226-17. - Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende.

Art. 226-18. - Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende.

Art. 226-18-1. - Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende.

Art. 226-19. - Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende.

« Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

Art. 226-19-1. - En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende le fait de procéder à un traitement :

« 1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;

« 2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

Art. 226-20. - Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende, sauf si cette

conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

« Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

Art. 226-21. - Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende.

Art. 226-22. - Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 EUR d'amende.

« La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 EUR d'amende lorsqu'elle a été commise par imprudence ou négligence.

« Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Protection juridique des Systèmes et des Données

Article 323-1 : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30000 euros d'amende

Article 323-2 : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-3 : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 226-15 : Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou

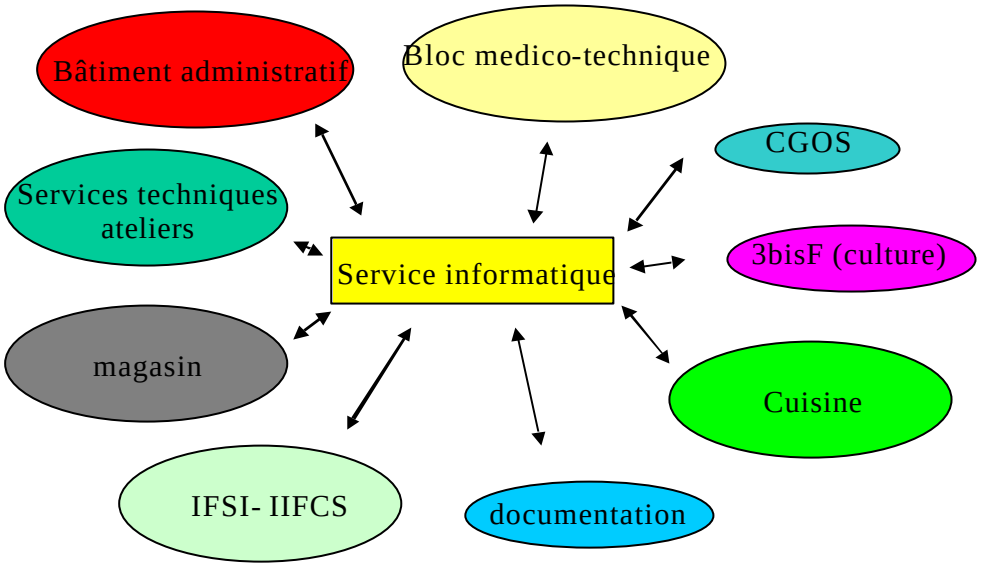
d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

.

ANNEXE III : SCHEMATISATION DU SYSTEME D'INFORMATION ACTUEL DU CH MONTPERRIN

Réseau informatique en « étoile »



Communication entre réseaux logiques