ENSP
ECOLE NATIONALE DE LA SANTE PUBLIQUE

RENNES

Directeur d'hôpital

Promotion 2002 - 2003

LA GESTION DU RISQUE INFORMATIQUE A l'HOPITAL : PROTECTION DE LA CONFIDENTIALITE ET SECURITE DES DONNEES AU CENTRE HOSPITALIER DE DREUX

Fabrice ORMANCEY

Remerciements

Je tiens à remercier Monsieur Jean-Marie DEGOIS, Directeur du Centre hospitalier de Dreux, pour l'accueil que j'ai reçu au sein de l'établissement et pour la confiance qu'il a bien voulu m'accorder au cours de mes stages.

Monsieur Pascal GOUIN, Directeur adjoint au Centre hospitalier de Dreux, a été un maître de stage attentif et a su jouer un rôle de compagnonnage tout au long de ma scolarité et à l'occasion de la réalisation de ce travail. Je lui en suis particulièrement reconnaissant.

Ce travail doit aussi beaucoup aux réflexions de Monsieur Michel RAUX, Directeur des systèmes informatiques au Centre hospitalier de Versailles, qui a accepté d'être l'encadrant de ce mémoire.

Enfin, je remercie Monsieur Alain KRATZERT, responsable du service informatique du Centre hospitalier de Dreux, qui a également largement contribué à la rédaction de ce mémoire. Dans une période chargée pour lui comme pour son équipe, il a toujours su prendre le temps de m'initier aux aspects techniques de la sécurité informatique.

Sommaire

Liste des sigles utilisés

ADSL	Asymetric digital subscriber line
AFNOR	Agence française de normalisation
AMDEC	Analyse des modes de défaillance, de leurs effets et de leur criticité
ANAES	Agence nationale d'accréditation et d'évaluation en santé
APR	Analyse préliminaire des risques
ARH	Agence régionale de l'hospitalisation
BS	British standard
CCAM	Classification commune des actes médicaux
CEN	Centre européen de normalisation
CH	Centre hospitalier
CHR	Centre hospitalier régional
CHU	Centre hospitalier universitaire
CIGREF	Club informatique des grandes entreprises françaises
CIHS	Conseil de l'informatique hospitalière de santé
CLUSIF	Club de la sécurité des systèmes d'information français
CNAMTS	Caisse nationale d'assurance maladie des travailleurs salariés
CNEH	Centre national de l'équipement hospitalier
CNIL	Commission nationale informatique et libertés
CPS	Carte de professionnel de santé
CRIH	Centre régional d'informatique hospitalière
CSIH	Conseil du système d'information hospitalier
CSP	Code de la santé publique
CSSIS	Conseil supérieur des systèmes d'information de santé
DCSSI	Direction centrale de la sécurité des systèmes d'information
DHOS	Direction de l'hospitalisation et de l'organisation des soins
DICOM	Digital imaging and communication in medicine
DIM	Département d'information médicale
DSIO	Directeur du système d'information et de l'organisation
EPS	Etablissement public de santé
FSE	Feuille de soins électronique
GEIE	Groupement d'intérêt économique européen

GHM	Groupe homogène de malades
GIE	Groupement d'intérêt économique
GIP	Groupement d'intérêt public
GMSIH	Groupement pour la modernisation des systèmes d'information hospitaliers
IGAS	Inspection générale des affaires sociales
ISA	Indice synthétique d'activité
ISO	International standard organization
LAN	Local area network
MCO	Médecine, chirurgie, obstétrique
NTIC	Nouvelles technologies de l'information et de la communication
PACS	Picture archiving and communication system
PMSI	Programme de médicalisation des systèmes d'information
RAID	Redundant array of inexpensive disks
RSA	Résumé de sortie anonymisé
RSIO	Responsable du système d'information hospitalier
RSS	Réseau santé social
RSS	Résumé de sortie standardisé
RSSI	Responsable de la sécurité du système d'information
SAMU	Service d'aide médicale urgente
SAN	Storage area network
SGBD	Système de gestion de bases de données
SIH	Système d'information hospitalier
SIR	Syndicat interhospitalier régional
SSII	Société de services et d'ingénierie informatique
SSO	Single sign on
VLAN	Virtual local area network

INTRODUCTION

Les établissements de santé sont des lieux où se concentrent des risques multiples et polymorphes. La mission de soins qui leur est confiée comporte elle-même des risques. Pour faire face à la maladie, y sont ainsi mises en œuvre des actions visant à apporter un bénéfice aux patients. Cependant, ces actions de soin comportent elles-mêmes des risques. Dans le domaine de la santé, ne pas prendre de risques conduirait en effet à ne pas soigner. Les professionnels de santé sont amenés dans leur activité à arbitrer en permanence entre des risques, en fonction des bénéfices attendus pour le patient.

S'il a pour vocation de limiter le risque de maladie, l'hôpital est donc aussi un lieu où en sont produits d'autres.

Les avancées technologiques et les organisations complexes qui les ont accompagnées ont permis des progrès considérables dans l'efficacité de la prise en charge des patients, mais ces gains ont aussi entraîné l'apparition de nouveaux risques. Les risques liés aux soins, tels que les infections nosocomiales et les erreurs médicales, sont les plus connus et les plus fréquents. Ainsi, aux Etats-Unis, le nombre de décès liés à une erreur médicale est estimé entre 40 000 et 100 000 par an, soit deux à trois fois plus que les accidents de la route. Les défaillances techniques sont plus rares mais peuvent avoir des conséquences tout aussi graves. Or, les usagers ne peuvent admettre qu'un établissement de santé où ils se rendent pour améliorer leur état de santé puisse devenir un lieu dangereux pour leur intégrité physique.

La gestion du risque est donc un enjeu majeur pour les établissements de santé et une préoccupation de plus en plus essentielle pour le directeur d'hôpital.

Définition du risque

Le risque peut se définir comme une situation non souhaitée ayant des conséquences négatives résultant de la survenue d'un ou de plusieurs événements dont l'occurrence est incertaine. Plus largement, il désigne tout événement redouté qui réduit l'espérance de gain ou d'efficacité dans une activité humaine. L'introduction au référentiel « Gestion de la qualité et des risques » de la dernière version du manuel d'accréditation des établissements de santé définit les risques comme « des événements qui mettent en jeu la sécurité des personnes et donc compromettent la réalisation des missions de l'établissement ».

La notion de risque a évolué au fil des siècles. Elle fait son apparition dans la culture occidentale à la fin du Moyen-Age et servait à désigner les écueils susceptibles de compromettre une bonne navigation. Elle constituait alors l'objet d'un contrat d'assurance.

Il faut attendre la fin du XIX^{e} siècle et le traitement de la question des accidents du travail pour que la notion prenne un plein statut juridique avec la catégorie du « risque professionnel », bientôt étendue à celle de risque social. Ce n'est que dans les années 1970 que la notion s'étendra et prendra son sens actuel. Certains, comme Ulrich Beck parlent même d'une « société du risque »[1]. Une nouvelle discipline, issue du monde de l'industrie et développée en France par l'Ecole des mines, a même fait son apparition, la cyndinique, ou science du danger.

Plus concrètement, le niveau de risque se mesure à partir de ses deux déterminants essentiels que sont la fréquence ou la probabilité de sa survenue et la gravité de ses effets ou de ses conséquences. Cette fonction est couramment utilisée dans les outils d'analyse des risques. Elle peut se résumer par l'équation suivante :

Risque = Fréquence x Gravité.

Sociologie du risque

Le risque ne doit pas être considéré uniquement de manière négative. Il fait partie de la vie et est présent dans toute activité humaine car la prise de risque est liée à la recherche d'un bénéfice dans l'activité réalisée. La prise de risque est souvent une condition de la performance. Dans tous les domaines, prendre des risques peut permettre d'augmenter la performance.

Le risque n'est pas uniquement une donnée objective, il est aussi une construction sociale. En effet, il recouvre un paradoxe : son acceptabilité est peu corrélée avec son intensité. C'est ainsi qu'alors que les accidents de la route font beaucoup plus de victimes que les catastrophes industrielles, ils sont beaucoup mieux acceptés.

Actuellement, la perception du risque se caractérise à la fois par une sensibilité exacerbée et par une apparente irrationalité. Un risque est davantage acceptable quand il est choisi et non subi, et surtout quand l'individu a le sentiment de pouvoir y échapper en mettant en œuvre sa capacité individuelle à le maîtriser. Bien que la mortalité liée à des risques subis n'ait jamais été aussi faible, la société contemporaine est ainsi perçue comme plus dangereuse que les précédentes. Cette perception se traduit par une demande d'efforts supplémentaires pour réduire les risques. Le sentiment d'insécurité apparaît supérieur à la réalité des menaces.

L'acceptabilité du risque est également variable en fonction de son type. Si les patients admettent encore parfois que puisse exister un aléa thérapeutique, donc un risque

[1] BECK U. *Riskgesellschaft, Auf dem Weg in eine andere Moderne*. Frankfurt, Suhrkamp, 1986

médical, ils considèrent que le risque technique doit être maîtrisé. La médecine est encore en partie considérée comme un art où il peut subsister une part d'incertitude. En revanche, la tolérance vis-à-vis de l'exposition aux risques techniques est très faible. Ceux-ci sont en effet l'occasion d'un danger absolument subi, auquel on ne s'expose pas volontairement et qui semble a priori résulter d'un défaut de vigilance de l'administration hospitalière à qui on a confié son sort. Les usagers du service public hospitalier ne peuvent donc pas accepter qu'une défaillance technique du système informatique puisse leur causer un quelconque préjudice.

Le risque informatique

Le système d'information comprend les informations qui sont collectées, gardées, traitées, recherchées ou transmises par une infrastructure informatique composée de matériels informatiques, d'équipements périphériques, de logiciels et de réseaux de télécommunication, ainsi que les ressources humaines qui l'organisent et le mettent en œuvre.

Cette définition permet de comprendre que le risque informatique consiste non seulement en un risque technique lié à la défaillance du matériel, mais qu'il consiste également par essence en un risque organisationnel, plus complexe à traiter et aux conséquences diverses. La sécurité des informations se mesure en effet à travers des caractéristiques essentielles que sont la confidentialité[2], l'intégrité[3] et la disponibilité[4], qui ne dépendent pas uniquement de la qualité de l'infrastructure technique mais également de nombreux critères qui relèvent de l'organisation de l'établissement. Aussi, le champ de la gestion du risque informatique comprend, outre la prévention des préjudices matériels et physiques, la prévention du préjudice moral lié à la divulgation ou à la perte de données sensibles et confidentielles.

Le SIH a ceci de particulier qu'il est vis-à-vis des risques un outil ambivalent. Il contribue tout d'abord à la maîtrise des risques lorsqu'il est utilisé pour assurer une meilleure traçabilité des procédures mises en œuvre à l'hôpital ou pour coordonner les activités des professionnels de santé. En contrepartie, il produit des risques en générant une

[2] propriété qui assure que seuls les utilisateurs habilités dans les conditions normalement prévues ont accès aux informations

[3] propriété qui assure qu'une information n'est modifiée que par les utilisateurs habilités dans les conditions d'accès normalement prévues.

[4] aptitude d'un système d'information à pouvoir être employé par les utilisateurs habituels dans les conditions d'accès et d'usage normalement prévues.

dépendance grandissante de ces mêmes acteurs du milieu hospitalier vis-à-vis d'un système de plus en plus ouvert et toujours plus complexe à maîtriser.

Longtemps moins développée que dans l'ensemble des entreprises et encore récemment cloisonnée à l'intérieur des établissements, l'informatique hospitalière se développe et les établissements de santé sont confrontés à l'ouverture croissante de leurs systèmes d'information dans trois directions.

1. À l'intérieur du système d'information de l'établissement, du fait du développement de l'appel à des services applicatifs communs et de la communication entre applications qui fonctionnaient précédemment en mode autonome.

2. Vers les systèmes d'information d'autres structures, au travers des coopérations interétablissements, des collaborations dans le cadre des réseaux de santé, des relations avec les médecins correspondants, pour mettre en œuvre le principe de prise en charge coordonnée du patient et la continuité des soins.

3. Vers le patient, qui devient un acteur du système d'information, notamment pour l'attribution de droits d'accès à son dossier médical lorsqu'il est informatisé.

Les modes de coopération interne et externe impliquent une plus grande maîtrise des risques d'atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes d'information de santé. De plus, les établissements de santé sont progressivement amenés à assumer de nouvelles responsabilités dans la gestion du système d'information, comme le respect de la vie privée du patient lors de l'utilisation des nouvelles technologies de l'information et de la communication, ou la traçabilité des opérations effectuées dans le système d'information.

La nécessité d'une gestion des risques à l'hôpital

La démarche de gestion des risques vise à concilier la prise de risque avec la maîtrise des dangers qui l'accompagnent, et donc à rendre le risque acceptable. Elle recherche un équilibre entre le bénéfice attendu et le risque accepté et repose sur la connaissance des risques, l'élimination de certains risques et la prévention et la protection vis-à-vis des risques à prendre de manière inéluctable pour la prise en charge du patient.

La prévention des risques hospitaliers a trois objectifs :

- Diminuer la fréquence et la gravité des incidents
- Améliorer la sécurité des patients
- Augmenter le niveau de qualité des pratiques.

La gestion des risques se structure peu à peu, et son champ s'élargit. Les risques liés aux dispositifs et aux gestes médicaux font depuis quelques années déjà l'objet d'une prévention renforcée :

- L'hémovigilance a pour objectif de « prévenir la survenue de tout effet inattendu ou indésirable résultant de l'utilisation thérapeutique des produits sanguins labiles[5] ».

- « La matériovigilance a pour objet la surveillance des incidents et des risques d'incidents résultant de l'utilisation des dispositifs médicaux[6] ».

- « La pharmacovigilance a pour objet la surveillance du risque d'effet indésirable résultant de l'utilisation des médicaments[7] ».

Les démarches qualité, notamment à travers les procédures d'accréditation, prennent en compte de manière de plus en plus importante la gestion des risques. L'ANAES, en diffusant en janvier 2003 des principes méthodologiques pour la gestion des risques en établissement de santé, encourage la mise en place d'une gestion centralisée de l'ensemble des risques pouvant survenir à l'hôpital. Il est ainsi reconnu qu'au-delà des risques liés aux activités de soin existent d'autres types de risques.

La gestion du risque devient ainsi un levier essentiel du management des établissements qui doivent mettre en place une véritable politique dont l'objet est de diminuer la fréquence de survenue des événements indésirables et, lorsque ces événements n'ont pu être évités, de diminuer leur impact. Le but est d'inspirer la confiance au personnel et aux usagers de l'établissement.

La responsabilité du Directeur d'hôpital en matière de gestion des risques

S'il n'est pas raisonnable de lui imposer la réduction à néant de l'ensemble des risques, on pourrait à juste titre reprocher au Directeur d'hôpital de ne pas avoir pris en compte un risque qui s'est concrétisé. Il s'agit donc pour lui de prévoir tous les moyens nécessaires pour réagir face à un incident et assurer la continuité du fonctionnement de l'hôpital.

Le Directeur d'hôpital se trouve cependant dans de nombreux cas face à des pressions contradictoires : la rigueur budgétaire d'un côté, et l'accroissement de la pression sécuritaire de l'autre. Il doit pourtant être d'autant plus vigilant qu'il semble que la sécurité s'apparente de plus en plus à une obligation de résultat et qu'elle devienne un impératif,

[5] art. R-666-2-1 du CSP
[6] art. R 665-48 du CSP
[7] art. R 5144-2 du CSP

voire un principe fondamental du service public hospitalier. Aucun domaine ne doit donc échapper à sa vigilance.

La nécessaire prise en compte de la gestion des risques liés au SIH

Le risque lié à l'utilisation des systèmes d'information est généralement oublié lors de la mise en place des politiques de gestion des risques. Toutefois, les menaces sont bien réelles. L'actualité illustre régulièrement les menaces qui pèsent sur les systèmes informatiques et les réseaux. L'été 2003 a été particulièrement marqué par la diffusion de codes pernicieux. La tendance générale est d'ailleurs à une progression constante de la sinistralité informatique. En 2002, en France, 26,3 % des entreprises ont été infectées par virus, alors que 14,8 % l'avaient été en 2001. 22,6% d'entre elles ont perdu des services essentiels, contre 16,9 % l'an passé. Chaque année, la CNIL établit un rapport sur la protection des données personnelles et insiste souvent sur la protection des données de santé, données considérées comme particulièrement sensibles. Dans son 12e rapport, elle signale ainsi que « nonobstant la règle du secret médical et leur pratique déontologique, les médecins, personnels soignants et directeurs d'hôpital ne sont pas suffisamment sensibilisés aux problèmes de confidentialité et de sécurité ».

Les systèmes d'information devenant de plus en plus complexes et concernant la majeure partie des activités de l'hôpital, la gestion du risque informatique ne peut plus être ignorée par les directeurs d'hôpital et laissée aux informaticiens. Alors qu'elle faisait l'objet jusqu'à présent de l'empilage de quelques briques hétérogènes, elle doit désormais faire l'objet d'une véritable politique de sécurité. A partir de la définition de la DCSSI, le GMSIH définit cette politique de sécurité comme «l'ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les biens, en particulier les informations médicales sensibles, au sein d'un établissement de santé et lors de ses communications avec d'autres systèmes d'information de santé ou d'autres professionnels de santé (réseaux de santé, praticiens libéraux, autres établissements ». Son objet est donc particulièrement ambitieux dans des établissements qui, à la différence des établissements bancaires par exemple, n'ont pas encore pris pleinement conscience de la réalité de ces risques et dont la préoccupation prioritaire est légitimement, dans un contexte budgétaire restreint, la maîtrise des risques liés directement aux activités de soins.

Economie du mémoire

Ce mémoire traite uniquement des données informatisées, à l'exclusion des informations véhiculées par d'autres moyens tels que le téléphone ou le télécopieur.

L'étude part du cas du CH de Dreux qui voit, comme la plupart des CH, son système d'information se développer considérablement et s'ouvrir tant en interne que vers l'extérieur de l'établissement. Dans ce nouvel environnement, une étude de son exposition aux risques doit être réalisée.

Il sera ensuite exposé dans quelle mesure la sécurisation et la protection de la confidentialité des données recouvrent des enjeux stratégiques pour l'hôpital. Ces enjeux sont à évaluer dans la perspective du bouleversement des pratiques médicales liées aux possibilités fournies par les NTIC, mais aussi dans le contexte économique, budgétaire et juridique dans lequel évoluent les établissements de santé.

Enfin, les nombreuses méthodes de sécurisation des systèmes d'information doivent être confrontées à la pratique des établissements de santé et replacées dans le cadre d'une politique de gestion du risque informatique adaptée à chaque établissement. Dans le cas du Centre hospitalier de Dreux, cette politique doit être strictement dimensionnée mais évolutive.

1 LE CENTRE HOSPITALIER DE DREUX VOIT CROITRE L'EXPOSITION AUX RISQUES DE SON SYSTEME D'INFORMATION

Le SIH de l'hôpital de Dreux est à une période à la fois stratégique et dangereuse de son évolution. Dans un marché de l'informatique encore peu soucieux de la fiabilité et de la sûreté des biens qui sont produits, la liberté laissée aux dirigeants hospitaliers d'organiser leur système d'information ne garantit pas la sécurité des données qui y circulent. Dans ce contexte, le CH de Dreux procède à une opération de changement complet de ses solutions informatiques, ce qui est l'occasion de faire le point sur sa vulnérabilité.

1.1 Le développement de l'informatique à l'hôpital engendre des risques quant à la sécurité du système et des données

1.1.1 L'informatique est intrinsèquement un domaine générateur de risques

A) Le spectaculaire développement de l'informatique en fait un domaine encore non mature

Bien qu'elle fasse partie de notre environnement quotidien, l'informatique est une discipline à l'histoire encore extrêmement courte. Son développement peut se résumer en trois périodes.

a) La première période peut être comparée à « la préhistoire ».

Elle retrace ce qui va donner naissance à l'informatique et peut être vue comme la convergence de trois courants.

- la *notion d'algorithme* prend ses racines dans l'Antiquité. Elle a été formulée en Perse dès le IX^{e} siècle. Elle consiste à décrire précisément les processus nécessaires à la réalisation des calculs complexes. Cette notion ne sera réellement formalisée que onze siècles plus tard par Alan Turing en 1936 et Alonzo Church en 1944.

- la *mécanisation des opérations de calcul* a commencé au XVII^{e} siècle, notamment avec les travaux de Blaise Pascal en 1642, puis avec la machine à effectuer les multiplications de Leibniz en 1694.

- la *programmation* est vraisemblablement apparue au Moyen Age pour les carillons automatiques, où un tambour muni de picots déclenchait une séquence de frappes sur les cloches. Cette technologie s'est ensuite développée pour l'animation des automates et la commande des métiers à tisser automatiques.

La synthèse des trois courants fut réalisée par Charles Babbage qui proposa en 1840 les plans de sa machine analytique. Celle-ci est la première description d'une machine à calculer programmable.

b) La seconde période correspond en quelque sorte à la « période antique »

Les machines à calculer programmables étaient utilisées pour calculer les tables numériques civiles et militaires ainsi que pour effectuer des statistiques. Il s'agissait de réaliser de manière répétitive des séquences de calcul assez simples sur de grands volumes de données. La croissance de ces besoins fit passer ces machines de la technologie mécanique à l'électromécanique, puis à l'électronique en utilisant des tubes électroniques. Les premières machines à calculer programmables électroniques furent la machine ABC en 1939 et le calculateur ENIAC en 1947. Alan Turing formalisa la notion de calcul en 1936 en montrant que ces machines pouvaient être universelles, c'est-à-dire capables de réaliser n'importe quel calcul. Cette période s'achève avec la proposition de John Von Neumann de ranger les programmes dans la même mémoire que les données, donnant naissance à l'architecture de nos machines actuelles.

c) Enfin, la troisième période peut être considérée comme celle des « temps modernes ».

Les premières machines des années 1950 contenaient déjà tous les ingrédients nécessaires à la construction d'un ordinateur. Une formidable évolution technologique va leur donner la puissance, la fiabilité et la miniaturisation que nous leur connaissons. La première de ces mutations va se produire vers 1960 avec le développement des premiers ordinateurs à transistors au silicium. Ces composants vont donner à l'ordinateur une fiabilité qui va lui permettre d'être effectivement utilisé. Le développement des circuits intégrés, dont le premier exemplaire est dû à Jack Kilby de la société Texas Instruments en 1958, va permettre dès 1965 un nouveau pas dans l'augmentation de la complexité et de la fiabilité des ordinateurs.

Pendant les années 1960, le statut des ordinateurs va progressivement passer de celui de machines à effectuer des calculs à celui de traiter de l'information de toute nature. Des applications comme le traitement de texte et les bases de données vont apparaître. En 1971, Marcian Hoff de chez Intel conçoit le premier microprocesseur commercial, l'Intel 4004, réalisé sous la forme d'un seul circuit intégré. Cette technique va progressivement se développer pour s'imposer à partir des années 1990. A partir de l'apparition du microprocesseur Intel 4004, un rythme très rapide d'évolution s'est installé et s'est maintenu sans fléchir jusqu'à aujourd'hui. La complexité de ces machines est passée de 2800 transistors en 1971 à plusieurs dizaines de millions pour les microprocesseurs

modernes. Pendant la même durée, leur puissance de traitement est passée de 60 000 instructions exécutées par seconde à plus d'un milliard par les machines actuelles les plus puissantes. L'histoire des microprocesseurs sur les trente dernières années est certainement la plus formidable évolution technologique de l'histoire humaine tant en durée qu'en ampleur. Ce rythme effréné est appelé loi de Moore, du nom du directeur de la compagnie Intel qui a formulé en dès le début des années 1970 la perspective d'un doublement de la capacité des microprocesseurs tous les 18 mois. Cette prévision s'est depuis lors vérifiée. Cependant, l'extrapolation de cette «loi» se heurte à des limites d'ordre physique, et il se pourrait que la période de doublement des transistors dépasse désormais 18 mois car les problèmes à résoudre deviennent de plus en plus complexes.

Ce n'est qu'au début des années 1960 que sont apparues les premières connexions de terminaux distants à des ordinateurs. Ceci permit de partager les ressources informatiques entre plusieurs utilisateurs éventuellement éloignés géographiquement, à une époque où les ordinateurs étaient rares et chers. Les prémices de ce qui devait devenir le réseau Internet sont apparues en 1968 en Angleterre au National Physical Laboratory. Il s'agissait de l'aboutissement des idées développées depuis 1964 par les militaires américains dans un contexte de guerre froide. Pour mettre au point un réseau de communication capable d'interconnecter leurs bases militaires malgré la destruction probable de certains centres d'interconnexion en cas de guerre, un concept de réseau ne possédant pas d'autorité centralisée avait été imaginé. Il s'agissait d'un réseau maillé sur lequel transiteraient des paquets de données. A partir de 1969, le projet ARPANET[8] valide le concept. L'adoption de cette technologie par les universitaires et les chercheurs donna naissance aux précurseurs d'Internet.

B) Les données numériques sont de plus par nature difficiles à sécuriser

Ross Anderson[9] utilise l'exemple suivant. Soit une suite de chiffres qui représentent un document envoyé par Alice à Bob. Ces chiffres circulent sur Internet entre l'ordinateur d'Alice et celui de Bob, et il se trouve qu'ils passent sous les yeux de Charlie. Si Charlie copie la suite de chiffres, il obtient une copie de la lettre d'Alice absolument identique à celle reçue par Bob. Cette copie est si parfaite que la notion d'original disparaît : les deux copies sont originales. Pire encore, ni Alice ni Bob n'ont aucun moyen de détecter à partir

[8] Advanced research projects agency network

[9] ANDERSON R. *Programming Satan's Computer*, http://www.cl.cam.ac.uk/ftp/users/rja14/satan.ps.gz

de leurs exemplaires qu'une copie a eu lieu. Si Charlie intercepte le flux de chiffres destinés à Bob, puis le renvoie à Bob sous son propre nom, Bob n'a aucun moyen de savoir que le document provenait initialement d'Alice et non de Charlie. Si Charlie intercepte le flux de chiffres et le modifie avant de le renvoyer à Bob sous le nom d'Alice, Bob n'a aucun moyen de détecter que le document a été modifié entre Alice et lui.

En d'autres termes, quand on parle de données numériques, on peut dire que la copie est parfaite et indétectable, la modification est indécelable et l'attribution impossible.

C) Il semble que, dans ce développement, les préoccupations de sécurité soient restées secondaires.

L'architecture de nos ordinateurs elle-même privilégie la souplesse à la sécurité. Ce sont des machines de Von Neumann depuis 1949, ce qui signifie que les ordinateurs ne font pas de différence interne fondamentale entre les données qu'ils doivent traiter et les instructions numérisées pour les traiter. Les ordinateurs sont utiles parce qu'ils sont programmables et donc adaptables à différents problèmes. Mais ces programmes étant numérisés et gérés par la machine indifféremment des données numériques qu'ils doivent traiter, ils ont les mêmes propriétés : copie parfaite et attribution impossible, mais surtout modification indécelable. L'architecture de Von Neumann est plus souple et plus efficace que les architectures concurrentes, ce qui a conduit à son adoption universelle, mais cette souplesse se paie en termes de sécurité. Ross Anderson a ainsi pu dire que la sécurité informatique était un défi similaire à la programmation contre son gré de l'ordinateur de Satan.

1.1.2 La complexité croissante des systèmes rend la sécurisation difficile

A) La taille des systèmes augmente le risque d'existence d'une faille de sécurité

Plus il y a d'éléments et de tâches à accomplir, plus il y a de chances qu'au moins une faille existe. Le caractère modulaire des systèmes complexes aggrave le problème. Les ingénieurs fragmentent un problème complexe en de nombreux sous-problèmes plus simples. La modularité est nécessaire pour résoudre des problèmes difficiles, mais elle a aussi pour conséquence de multiplier les failles potentielles : chaque module, mais aussi chaque interaction entre plusieurs modules est le lieu potentiel d'une faille de sécurité et le nombre d'interactions augmente potentiellement avec le nombre de modules.

B) L'analyse des systèmes est de plus en plus difficile

Plus un système est grand, plus il est difficile à comprendre, à se représenter, à analyser. Au-delà d'une certaine taille, lanalyste ne peut plus avoir en tête une image mentale

complète et correcte du système, ce qui augmente la probabilité qu'une faille passe inaperçue. Or, il suffit d'une seule faille pour compromettre l'usage d'un système. La sécurité de l'ensemble est égale à la sécurité du maillon le plus faible.

1.1.3 Le marché de l'informatique commence seulement à s'intéresser à la sécurité et à la protection de la confidentialité

A) La sécurité a un coût élevé.

a) Le marché pousse à la complexité

Toujours plus de choix, plus d'options, plus de capacités, plus de fonctionnalités sont proposées aux acheteurs. Les décisions d'achat des ordinateurs se prennent en comparant des listes de fonctionnalités et la concurrence effrénée de ces marchés pousse chaque fabricant à rendre ses machines encore plus complexes, encore plus souples, encore plus puissantes, de ce qui entraîne l'obsolescence rapide des matériels installés. Les recherches des constructeurs s'orientent donc prioritairement vers l'ajout de fonctionnalités nouvelles, qui permettent de dégager un avantage comparatif par rapport à la concurrence quitte à sacrifier parfois un peu de fiabilité.

b) Améliorer la sécurité d'un système coûte cher.

Cela requiert en effet des études très poussées, des analyses coûteuses. Or, le résultat n'est pas garanti, car la sécurité ne se prouve pas. Les fabricants n'étant jamais certains de la sécurité de leurs systèmes et ne pouvant pas se targuer de celle-ci, la sécurité de leurs produits n'est pas un argument de vente. Elle est donc maintenue au minimum acceptable par le client.

c) Cependant, les constructeurs commencent à se préoccuper du niveau de sécurité de leurs produits.

Deux cents industriels du secteur informatique, dont Intel, Microsoft, IBM, Hewlett-Packard, se sont réunis depuis 1999 au sein d'un consortium, « l'Alliance pour une informatique de confiance » (Trusted Computing Platform Alliance). L'objectif affiché de ce regroupement est d'établir les standards matériels garantissant une informatique « intègre », respectant la confidentialité des communications. L'essentiel de ces travaux concerne la mise en place d'un module de sécurité contenant des informations de chiffrement, intégrées à de nouvelles générations de puces. Ces efforts récents visent prioritairement à sécuriser les échanges dans l'optique de développer le commerce électronique, mais ils sont significatifs d'une prise de conscience de la faiblesse du niveau

de sécurité des produits informatiques existant à l'heure actuelle et du besoin de susciter davantage de confiance de la part des utilisateurs.

B) Le marché des produits de sécurité se développe rapidement

a) Le sentiment de vulnérabilité s'est récemment accentué

A la suite du passage à l'an 2000 et des attentats du 11 septembre 2001, beaucoup d'organismes ont pris conscience de leur vulnérabilité. L'enquête du CLUSIF sur la sinistralité informatique en France fait ainsi ressortir une baisse significative du sentiment de confiance des entreprises quant à la qualité de la protection de leurs systèmes informatique. Ainsi, alors que 41% des entreprises s'estimaient très bien protégées en 2001, elles ne sont plus que 17% en 2002.

b) Le marché de la sécurité est en plein essor

En France, le marché de la sécurité est évalué en 2002 à 11,2 milliards d'euros, en progression de plus de 9%. Parmi les postes qui se développent le plus, on retrouve la sécurité informatique, qui progresse de 16,2 %. Ce marché va sans doute encore se développer puisque 37% des entreprises envisagent de développer prochainement leur budget de sécurité informatique. C'est le cas de 62% des établissements hospitaliers.

C) La gestion des risques, et notamment du risque informatique, commence à faire son entrée dans les programmes des grandes écoles d'ingénieur et de management

Les grandes écoles élaborent et intègrent dans les programmes de nouvelles méthodes et de nouveaux contenus permettant de réagir au mieux aux risques de tous ordres. L'enseignement de la gestion des risques est encore émergent. Ces cours sont rarement enseignés de manière globale et transversale et restent souvent au niveau de la sensibilisation. La sécurité informatique est ainsi enseignée au niveau de la prévention des risques et peu au niveau de leur gestion. Dans la plupart des grandes écoles d'ingénieur en informatique, les cours sur les systèmes d'information, les réseaux ou les protocoles sont émaillés de notions sur la fiabilité des composants, des logiciels, sur les failles de sécurité et les réflexes de base. Mais la matière intéresse peu les étudiants, et les options spécialisées sur la sécurité attirent peu d'audience. De même, les ingénieurs reçoivent peu d'enseignements en sciences humaines et sociales, ce qui empêche la capacité d'analyse des erreurs humaines et d'organisation, principaux facteurs de risques. En revanche, les écoles de management développent désormais largement un enseignement approfondi sur la gestion des risques.

La prise de conscience du faible niveau de sécurité offert par les matériels informatiques, les logiciels et la circulation des données sur les réseaux est donc récente. Les établissements de santé n'ont eu que peu à s'inquiéter de cette situation étant donné leur faible niveau d'exposition au risque jusqu'à aujourd'hui. La libéralisation de la politique d'informatisation des hôpitaux a cependant changé complètement ce contexte.

1.2 Les hôpitaux, désormais libres d'organiser leur système d'information, doivent prendre en charge sa sûreté de fonctionnement et la protection des données

1.2.1 Le développement de l'informatique est demeuré très encadré jusqu'à la fin des années 1980

A) Une informatique balbutiante et régionalisée dans les années 1960

a) Une informatique encore embryonnaire

Dans les années 1960 apparaissent les ateliers mécanographiques dans les centres hospitaliers régionaux. On y trouve le matériel et les logiciels permettant de répondre aux besoins élémentaires de gestion d'un établissement de taille importante, que ce soit la paie du personnel, la comptabilité ou la facturation des séjours des malades. Il ne s'agit cependant pas encore de gestion. Les applications sont purement locales, les traitements sont réalisés avec des trieuses traitant des milliers de cartes perforées sur lesquelles se trouvent les informations. Celles-ci sont saisies par des pools de dactylo-codeuses et exploitées par les opérateurs qui sont à l'origine des premières générations d'informaticiens.

b) Une politique de développement de l'informatique hospitalière se met en place

Pour réaliser une meilleure rentabilité des investissements et pour améliorer l'efficacité et la sécurité du service public, l'interconnexion des matériels apparaît comme la solution la plus économique. La création d'ateliers interhospitaliers dans les CHR est encouragée afin de réaliser des économies d'échelle. Cette politique vise également à réunir et à exploiter sur le plan national des statistiques complètes et diversifiées de manière à définir une politique sanitaire. La circulaire encourage donc le développement de l'informatique et le choix des matériels dans le cadre de ces perspectives. Au total, la tutelle est donc renforcée afin de veiller à la cohérence du traitement des informations et de limiter la redondance des développements.

c) Un embryon d'informatisation des hôpitaux

Une circulaire de 1966[10] va permettre à tous les établissements d'accéder aux traitements de l'information. Il ne s'agit cependant que de traitements en temps différé, sans saisie directe par les utilisateurs. Ces traitements sont centralisés sur un seul site d'exploitation, celui du CHR.

B) Une informatique qui ne répond plus aux besoins des hospitaliers dans les années 1970

a) Les établissements hospitaliers sont insatisfaits

Les produits informatiques sont des produits locaux, réalisés avec des techniques anciennes, qui devront être revus pour fonctionner sur la nouvelle génération de matériel. Ils ne permettrent pas de répondre aux besoins de l'ensemble des établissements hospitaliers. La solution retenue par les établissements est alors souvent d'utiliser les services bureaux proposés par les constructeurs tandis qu'une offre informatique nationale que le gouvernement désire voir se développer est en train d'apparaître.

b) Un double contrôle qui mécontente les utilisateurs

Les tutelles régionales sont renforcées[11]. Les CHR contrôlent le développement de l'informatique des Centres hospitaliers qui ne doivent plus passer par les services bureaux des constructeurs et doivent consulter le directeur régional du CHR de leur région pour l'étude des solutions possibles aux problèmes posés par l'informatisation. Les ateliers interhospitaliers vont se transformer en Centres régionaux d'informatique hospitalière (CRIH). Cette tutelle régionale entraîne un mécontentement croissant des directeurs de CH vers la fin des années 1970. En effet, dans les établissements, il n'existe pas de véritable interlocuteur et l'informatique reste l'affaire des informaticiens du CHR. A ce contrôle régional s'ajoute un contrôle de tutelle national qui ralentit le traitement des dossiers informatiques et ne permet pas de répondre correctement aux demandes de plus en plus nombreuses des utilisateurs.

c) Le passage au traitement conversationnel

Des applications nationales sont développées et utilisées par la presque totalité des structures régionales qui en assurent ainsi la production pour l'ensemble des

[10] Circulaire n°266 du 25 octobre 1966

[11] Circulaire n°52 du 17 avril 1970

établissements de France. Mais les utilisateurs souhaitent voir se développer des fonctions de gestions. Les structures régionales les plus dynamiques vont ainsi développer autour de ces applications nationales des applications de gestion et même les remplacer, multipliant ainsi sur l'ensemble du territoire des produits de même nature. Les établissements les plus importants se dotent d'écrans dits passifs, en lien direct avec leur structure régionale. Ainsi, il est possible de saisir les informations à la source, ce qui limite les risques d'erreurs.

C) L'apparition des premiers systèmes d'information hospitaliers dans les années 1980

a) De nouveaux produits voient le jour

Le développement de nouvelles applications par certains CRIH a entraîné une profonde disparité des niveaux d'informatisation des établissements entre les différentes régions et une hétérogénéité des systèmes qui va à l'encontre des objectifs initialement poursuivis et met en péril la cohérence des informations transmises aux différents partenaires de l'hôpital. L'informatique demeure extérieure à l'activité quotidienne de l'hôpital. Elle reste une affaire de spécialistes et le traitement des malades n'a pas directement bénéficié des outils mis en place. Le développement de l'informatisation des fonctions de soin nécessiterait une exploitation au niveau de l'établissement du fait de la spécificité des données médicales qui demande une protection de la confidentialité et parce que le volume considérable de données à traiter dépasserait les capacités de stockage et de traitement des CHR. De plus l'approche informatique de l'hôpital a été réalisée à travers le traitement spécifique de telle ou telle fonction sans qu'ait pu aboutir une mise en cohérence technique et fonctionnelle de l'ensemble.

b) La décentralisation

Deux éléments vont se conjuguer pour permettre l'autonomisation des établissements. Tout d'abord, l'évolution technologique, avec l'apparition des techniques de base de données et des réseaux qui permettent de construire une informatique cohérente sur le plan technique et en accord avec la politique et les objectifs globaux des établissements. Ensuite, la baisse des coûts des ordinateurs qui va mettre à la portée de davantage d'établissements une informatique autonome.

La notion de filières est entérinée[12]. L'analyse des traitements de l'information à l'hôpital fait en effet apparaître des besoins communs à des groupes d'établissements. La nécessité d'une coopération interhospitalière, pour répartir les coûts d'investissement et pour réaliser des systèmes informatiques performants, conduit à promouvoir des solutions valables pour des groupes d'établissements semblables. Vers le milieu des années 1980, la décentralisation est devenue irréversible.

c) L'inflation des moyens informatiques dans les établissements

Il n'appartient plus aux CRIH de définir les objectifs de l'informatisation des établissements. Ils doivent seulement proposer des solutions techniques et évaluer les moyens qui les rendent opérationnelles. Cette nouvelle autonomie se traduit par une inflation des moyens informatiques dans les établissements hospitaliers et s'accompagne d'une augmentation du personnel informaticien. Ainsi entre 1989 et 1990, cette catégorie de personnel augmente de 44%. En outre, le taux de croissance des dépenses informatiques des établissements s'élève à 36% entre 1984 et 1985. Au milieu des années 1980, 1,16% du budget de fonctionnement des hôpitaux sont consacrés à l'informatique)

1.2.2 Un marché en complète révolution dans les années 1990

A) Le grand bouleversement de l'informatique hospitalière

a) Les faiblesses de l'informatique hospitalière au début des années 1990

L'informatique hospitalière, au début des années 1990, reste encore rivée sur les filières nationales, en grande partie obsolètes et dépassées. Elle ne prend guère en compte l'évolution des technologies, en particulier le développement des réseaux. Elle reste tournée vers l'informatique administrative et a tardé à prendre en compte l'ensemble du système d'information de l'hôpital. Les applications médicales résultent de développements locaux et sont déconnectées des applications liées à l'informatique de gestion. De leur côté, les pouvoirs publics exercent encore une forte tutelle sur les décisions des établissements.

b) La révolution informatique

Le marché de l'informatique va connaître une complète révolution. De nouvelles technologies voient le jour, les solutions propriétaires perdent de leur importance, ce qui

[12] Circulaire n°16 du 18 novembre 1982

supprime le lien technique qui justifiait les filières. Les offres de solutions fonctionnent de plus en plus avec un Système de gestion de bases de données du marché et avec un système d'exploitation standardisé (par exemple UNIX). La concurrence peut donc se développer.

c) L'ouverture du marché[13]

Les hôpitaux sont tenus de réaliser un schéma directeur informatique dans le cadre de leur projet d'établissement et ont le libre choix des solutions à mettre en œuvre, tant du point de vue matériel que du point de vue applicatif. Le marché de l'informatique hospitalière passe d'un marché semi-protégé avec interventionnisme de l'Etat à un marché libre où l'offre est le fait des structures hospitalières informatiques (SIR, CRIH), de sociétés de services spécialisées ou non dans le domaine public, de sociétés spécialisées dans le domaine des cliniques privées et qui adaptent leur offre au domaine public et de sociétés disposant d'une offre dans le domaine public, par exemple celui des collectivités locales et quoi l'adaptent au contexte hospitalier public. Devant cet accroissement de la concurrence, le marché va se réguler grâce à l'encouragement de la normalisation, à la coopération public privé dans le cadre de GIE et GEIE entre les CRIH et des industriels et à la constitution de grands pôles privés de niveau international

B) Depuis les années 1990, les tentatives de structuration du marché de l'informatique hospitalière se multiplient

a) Dans un marché déréglementer, l'Etat se veut régulateur[14]

Il est créé auprès du ministre chargé de la Santé une instance de concertation spécialisée dans le domaine informatique hospitalière et associant les différents acteurs du système hospitalier : le Conseil de l'informatique hospitalière et de la santé (CIHS). Chaque établissement doit déterminer le développement de son informatique de manière cohérente au plan interne et avec l'environnement existant. L'Etat contrôle le schéma directeur du système d'information et de l'informatique.

b) La volonté de structurer le marché

Depuis 1989, l'informatisation hospitalière est basée sur les principes de responsabilité et d'autonomie des établissements. Si ce système a permis d'accroître les moyens

[13] Circulaire n°275 du 6 janvier 1989

[14] Circulaire n°28 du 19 avril 1991

informatiques dans les hôpitaux, il a aussi contribué à la dispersion des crédits consacrés à l'informatique, à une prolifération des solutions incompatibles avec la taille et la nature du marché hospitalier, voire à une déstructuration du SIH. D'où la volonté des pouvoirs publics, tout en respectant les principes d'autonomie et de liberté de choix des établissements de mettre en place une régulation basée sur la normalisation des systèmes et le renforcement des compétences des décideurs hospitaliers. Une circulaire 25 décembre 1995 relative à la normalisation des systèmes d'information hospitaliers vise ainsi à structure le marché par une meilleure organisation de la demande. L'Etat se voit attribuer 3 rôles essentiels : effectuer une analyse stratégique, développer la prospective, évaluer la mise en œuvre de l'informatique hospitalière. Il est à noter que pour la première fois la sécurité de l'information apparaît comme un objectif dans les textes officiels.

c) L'état des lieux à la fin des années 1990 : un marché libre

Le marché de l'informatique hospitalière actuel est un marché encore peu étudié et mal connu. Les offres en matière de SIH portent encore le poids de l'histoire. Il est en effet remarquable que la logique de filière tend à persister et que les fournisseurs raisonnent toujours en termes de modules séparés. Les établissements peuvent encore choisir d'acquérir chacune de ces briques séparément chez des éditeurs différents. On ne peut donc pas parler de système d'information unique mais de systèmes d'information au pluriel dans lesquels on distingue la gestion économique et financière (GEF), la gestion administrative du malade (GAM), la gestion des ressources humaines (RH), etc. Cette façon de penser le SIH ne facilité pas sa cohérence, ni sa parfaite intégration. Malgré l'ouverture du marché à la concurrence, les offres n'ont pas encore parfaitement intégré un besoin essentiel des établissements de soins : le patient doit être placé au centre du système d'information. Les fournisseurs ne sont pas les seuls à blâmer. Les professionnels de santé portent eux aussi leur part de responsabilité parce qu'ils n'ont pas été à même de définir leurs besoins de façon suffisamment cohérente. Depuis plus de vingt ans, la définition d'un dossier commun du patient structuré et convenant aux différents spécialistes est à l'étude sans qu'aucune tentative n'aboutisse. Le suivi de la réglementation qui le définit est de surcroît compliqué par les fréquentes modifications qu'elle connaît. L'article du CSP portant sur les modalités de sa communication a par exemple été modifié quatre fois en six ans. En l'absence de référentiels et de normes sémantiques adoptées par tous, il est compréhensible que les industriels ne se précipitent pas dans le développement de solutions dans ce domaine. La reconnaissance de la nécessité de recentrer les systèmes d'information autour du patient et de créer des systèmes d'information qui dépassent le cadre des hôpitaux va sans doute contribuer à encore faire évoluer les offres.

C) La conséquence de cette évolution est une plus grande exposition aux risques

a) Une vulnérabilité ressentie par les acteurs du monde hospitalier

Cette exposition grandissante aux risques résulte du double mouvement d'extension et de décloisonnement du système d'information en interne et de l'ouverture du système au-delà de l'enceinte de l'hôpital. L'enquête du CLUSIF sur la sinistralité en 2002[15] montre que l'ouverture des systèmes d'informations est une réalité. En effet, 50% des hôpitaux possédaient un réseau Intranet en 2002, et 41 % disposaient d'une ouverture sur Internet. Ces chiffres peuvent paraître faibles, mais l'enquête porte sur l'ensemble des établissements, y compris les plus petits. L'exposition au risque est désormais relativement importante pour les établissements hospitaliers. L'enquête montre une prise de conscience de cette vulnérabilité, ce qui est nouveau. 41 % des dirigeants hospitaliers estiment que leur établissement est fortement dépendant de son système d'information.

b) La sinistralité reste à des niveaux peu élevés dans les hôpitaux

L'enquête citée ci-dessus, réalisée par le CLUSIF, fait état d'une sinistralité relativement faible. Ainsi, près de deux tiers des établissements ne déclarent aucun incident. Les causes des sinistres constatés sont pour 36% des infections par virus, pour 29% des pertes de services essentiels, pour 27% des erreurs d'utilisation et pour 15% des pannes internes. Ces causes sont donc avant tout internes, même si les enquêtés ont sans doute eu tendance à minorer la sinistralité due aux accidents physiques, aux fraudes ou aux intrusions. Plusieurs raisons peuvent expliquer ces résultats. En premier lieu, il faut noter que cette étude est basée sur le principe de l'enquête et que les établissements sont toujours réticents à faire état de leurs faiblesses. Ensuite, il importe de rappeler que les systèmes d'information hospitaliers se sont ouverts très récemment et le sont encore relativement peu, comparés à ceux des entreprises du secteur privé qui, bien que l'enjeu de l'image de marque soit supérieur à celui des hôpitaux, déclarent un peu plus de sinistres. Enfin, la faiblesse des attaques externes peu s'expliquer par le peu de motivations financières qui existent dans l'attaque des systèmes d'informations des établissements de santé. D'une part, en raison des règles de la comptabilité publique. La séparation de l'ordonnateur et du comptable a pour conséquence que les enjeux du détournement de fonds se situent davantage dans le système d'information du Trésor Public. D'autre part, les systèmes d'information hospitaliers ne sont, comme nous l'avons vu, que peu centrés sur le patient. Les informations circulant sur les systèmes

[15] CLUSIF, *Etude et statistiques sur la sinistralité en France, année 2002*, http://www.clusif.asso.fr

informatiques hospitaliers sont essentiellement administratives ou concernent des résultats d'actes médico-techniques. Les données qui circulent ont donc peu de valeur pour les éventuels pirates informatiques. L'informatisation des dossiers des patients risque cependant de rendre les données plus sensibles et de leur donner davantage de valeur financière.

1.2.3 Dans le nouveau contexte qui est le leur, les hôpitaux se trouvent largement désemparés face à l'absence d'organisation des acteurs intervenant dans le secteur de la sécurité informatique

A) Les systèmes d'information encouragés par les pouvoirs publics sont inachevés et en partie dépassés

Les pouvoirs publics ont pris conscience des possibilités offertes par l'informatique dans le milieu de la santé et ont compris que la sécurisation des données représentait la condition incontournable de l'utilisation des NTIC. Des initiatives qui auraient pu constituer le socle de systèmes d'information sécurisés performants ont donc été encouragées. La lenteur de leur mise en application a cependant condamné leur généralisation.

a) Le Réseau Santé Social (RSS)

Le RSS est un réseau de transport de l'information basé au départ sur le réseau téléphonique commuté. Le choix de l'opérateur sur ce réseau s'est porté sur Cegetel le 31 décembre 1997. La technologie utilisée est un Intranet reliant les réseaux de l'Assurance maladie, des régimes complémentaires et des établissements de soins, associé à un Extranet avec les professionnels de santé. Le RSS est réservé aux professionnels de santé. Ne peuvent utiliser le RSS que les porteurs de carte CPS. Cette ouverture restreinte permet donc à ce réseau de limiter les risques sécuritaires. De plus, trois procédures de sécurisation permettent la protection des données échangées. Tout d'abord, une authentification à la source et une signature, puisque toute personne pénétrant sur le RSS est identifiée par sa carte CPS. Ensuite, un chiffrement des données. Enfin, des systèmes de sécurité utilisant des firewalls sur l'ensemble des accès garantissent la non-intrusion d'utilisateurs ne faisant pas partie des abonnés professionnels de santé et protégent le réseau contre les virus.

Le RSS a été vu dès sa conception comme un outil de relation avec les caisses d'assurance maladie. Il devait permettre le traitement sans papier des feuilles de soins. Le RSS a ensuite été vu comme un outil d'accès à la connaissance et à la communication entre professionnels. Il n'intègre pas la relation avec les patients. Cependant, le contexte technologique et institutionnel a changé depuis la mise en place du RSS. Ce réseau est

donc porteur d'un cloisonnement qui n'est plus indispensable aujourd'hui pour réaliser des échanges de données confidentiels et sécurisés. Le RSS n'a pas le monopole des connexions pour le transfert des FSE. D'autres sociétés se sont lancées dans l'offre de réseaux sécurisés à destination des professionnels de santé et offrent des alternatives pour la constitution de réseaux de télémédecine. Le RSS propose aujourd'hui peu de services (messagerie électronique médicale sécurisée, transmission de feuilles de soins électroniques, quelques sites médicaux), tandis que des offres se développent rapidement sur Internet. Il est également porteur d'un cloisonnement. Son avenir semble donc limité à brève échéance, d'autant plus que le coût de son utilisation est élevé et que les évolutions techniques sont bridées par sa licence.

b) La carte CPS

La CPS est une carte à puce permettant au professionnel de santé d'authentifier, c'est-à-dire de signer, la FSE et d'assurer la sécurité des transactions. La carte permet au titulaire de s'authentifier vis-à-vis du RSS. Il peut ensuite signer les FSE et transmettre les informations administratives et médicales. C'est la signature du praticien qui a effectué l'acte. La CPS est déclinée dans les différentes professions médicales et paramédicales.

Le GIP CPS chargé d'émettre, de gérer et de promouvoir la CPS est né le 5 février 1993. La CNAMTS assure plus de 80% de son financement. A l'origine, l'instauration de cet outil présentait l'intérêt de mettre en place un annuaire des professionnels de santé complet et mis à jour. Cet annuaire est une pièce essentielle dans la constitution d'un système d'information sécurisé. Le rapport de l'IGAS de novembre 2002 a cependant montré que la mise en place de la carte CPS n'a pas permis de réduire le nombre de fichiers de professionnels de santé et qu'elle n'a pas non plus permis d'améliorer leur exhaustivité et la qualité des informations qu'ils contiennent.

La carte CPS a plusieurs fonctions. Elle permet l'authentification des professionnels pour l'ensemble des échanges de santé, mais assure aussi la fonction de signature électronique et celle de chiffrement. Ces fonctions de signature électronique et de chiffrement sont toutefois peu ou pas utilisées en raison de la lourdeur et de la lenteur des procédures.

La carte CPS est, en dépit de ses insuffisances, un outil majeur qui peut être intégré dans une politique de sécurité des établissements de santé, mais son utilisation reste faible en milieu hospitalier, mises à part quelques initiatives expérimentales telle que celles du CHU de Strasbourg, du CH de Macon ou de l'Institut mutualiste de Montsouris. Ce faible déploiement tient en grande partie au coût qu'il représente pour les établissements. Le coût de la carte est en effet élevé, compris entre 15 et 23 euros par an. De plus, d'autres

techniques, plus souples, moins coûteuses et plus performantes sont proposées par des sociétés privées spécialisées dans le domaine de la sécurité.

c) La carte SESAM-VITALE

La carte SESAM-VITALE II est en voie d'individualisation. Elle doit devenir individuelle pour toute personne en 2006. Elle comporte un volet administratif et amène une simplification des procédures dans la gestion des feuilles de soins électroniques (FSE). La voie d'une carte porteuse du dossier médical du patient s'est avérée être une source de difficultés techniques et pratiques. Les résistances à sa mise en place tiennent à trois raisons majeures. En premier lieu, les lecteurs de cartes compatibles ne faisant pas partie de l'équipement standard des micro-ordinateurs, leur disponibilité entraîne un surcoût pour le professionnel comme pour le patient. En second lieu, la réflexion sur les techniques à utiliser pour ouvrir des accès aux informations individuelles doit se situer au niveau international et non au niveau de la France uniquement. Les compagnies d'assurance des voyageurs pourraient être sollicitées pour le financement des données partagées si les choix technologiques restent ouverts et non spécifiques au territoire national. Pour l'instant, ce matériel n'est en effet pas disponible dans les autres pays.

B) Les acteurs intervenant dans le domaine de la sécurisation des SIH sont encore trop peu efficaces

a) L'Etat ne joue pas son rôle de régulateur en matière de sécurité des systèmes d'information hospitaliers

Les organismes ayant pour mission de guider ou de mettre en place les systèmes d'information en santé sont parfois inexistants, souvent éphémères ou redondants quand ils ne sont pas concurrents.

La disparition du Conseil de l'informatique hospitalière de santé (CIHS) en 1998 a ainsi été décidée sans que la mise en place du Groupement pour la modernisation du système d'information (GMSIH) soit effective. Le GMSIH n'a été constitué qu'en mars 2000. Pendant plus de deux ans, la mise en œuvre d'une politique dans ce domaine n'a été confiée à aucune structure. De même, le Conseil supérieur des systèmes d'information de santé (CSSIS) mis en place en 1997 n'a pas été renouvelé en 2000. Aucune structure de remplacement n'a été mise en place.

La dynamique d'informatisation du système de santé a par ailleurs été affaiblie. Le passage d'une politique dirigiste à une politique d'ouverture du marché hospitalier aux industriels a été réalisé sans préparation des décideurs aux enjeux des systèmes d'information orientés vers la prise en charge des patients. En même temps, le mode de

financement des hôpitaux a changé, polarisant les esprits et les moyens sur la production d'indicateurs économiques élaborés à partir d'informations médicales saisies le plus souvent dans ce seul objectif. Le lancement puis la généralisation du PMSI a favorisé le développement de systèmes d'information «verticaux » ne prenant pas en compte la nécessaire transversalité de la collecte et du traitement de l'information pour répondre à la finalité primordiale : la continuité des soins. D'autres systèmes d'information demandés par le ministère ou les agences, sur les traçabilités et les vigilances par exemple, ont été mis en place sans une approche du dossier du patient. Ces systèmes d'information comportent un défaut conceptuel important : ils sont centrés métiers ou centrés service, mais pas centrés patient. De ce fait, ils produisent des données de qualité médiocre et engendrent des risques d'erreur.

Au total, de nombreuses institutions interviennent pour exiger ou recommander la mise en place de systèmes d'information, sans que la cohérence d'ensemble soit assurée.

Il ne faudrait pas en déduire que l'Etat n'a pas de rôle à jouer dans ce domaine. Toutefois, son rôle est d'être régulateur, et non opérateur. Le GMSIH, constitué sous forme de GIP dans lequel l'Etat est représenté aux côtés notamment des établissements de santé, vise à assurer cette fonction de régulation. Il a été créé par un arrêté du 23 février 2000 avec pour objectif de structurer la demande hospitalière à travers des spécifications communes et des standards de communication stables. Il comprend aujourd'hui plus de 500 adhérents publics et privés. Sa mission est de concourir, dans le cadre de la construction du système d'information de santé, à la mise en cohérence, l'interopérabilité, l'ouverture et la sécurité des systèmes d'information utilisés par les établissements de santé. La DHOS quant à elle n'intervient pas dans le domaine des systèmes d'information. Elle aurait pourtant un rôle à jouer dans le domaine de la normalisation et de l'élaboration de standards communs en relation avec le GMSIH. L'Etat commence néanmoins à vouloir jouer son rôle par l'intermédiaire de ses correspondants régionaux au niveau des ARH, qui réfléchissent sur les moyens de mettre en place des réseaux régionaux de santé.

b) Le rôle du secteur privé

Les établissements de santé disposent d'une autonomie de gestion importante en matière de structuration de leurs systèmes de santé. Or, dans un domaine aussi technique et spécifique que celui-ci, tous ne disposent pas des compétences nécessaires en interne et n'ont d'ailleurs, pour la très grande majorité, pas vocation à en disposer.

Le recours aux compétences du secteur privé est donc encouragé dans ce domaine. Il peut s'agir de faire appel aux ressources des associations spécialisées dans le domaine

de la sécurité informatique, comme le CLUSIF ou le CIGREF. Ces associations dispensent des conseils, élaborent et diffusent des guides de bonnes pratiques et des méthodes de sécurisation à tous les organismes qui le souhaitent. Au côté de ces associations, les SSII et les sociétés de conseil ou d'audit proposent des services plus ou moins complets dans le domaine de la sécurité des systèmes d'information, auxquels il peut être recouru pour pallier les insuffisances de moyens internes ou pour contrôler le niveau de sécurité existant.

C) La grande liberté laissée aux responsables des SIH dans la sécurisation des systèmes et des données

a) Il n'existe pas de réglementation relative à l'élaboration de systèmes d'information sécurisés

De manière générale, les hôpitaux sont soumis à une évolution de la réglementation de leurs activités d'une densité telle qu'il est très difficile de pouvoir y satisfaire et qui entraîne par ailleurs les établissements dans des situation à risque de non-respect de la législation. Cette réglementation concerne tout particulièrement les activités de soin, mais aussi les domaines techniques. Il existe ainsi une réglementation précise relative à la sécurité incendie, à la sécurité électrique, mais aussi en matière de sécurité environnementale (eau, air, gestion des déchets) et de sécurité alimentaire. Cette réglementation s'est développée depuis le début des années 1990 plutôt de façon réactive et a posteriori, de manière cloisonnée. Cette approche explique peut-être en partie le fait que la sécurité des systèmes d'information n'a pour l'instant pas fait l'objet d'une telle prise en compte au niveau réglementaire. La relative faiblesse de la sinistralité actuelle dans les établissements de santé n'a pas rendu nécessaire la réglementation de ce domaine.

La législation relative aux droits des patients et aux responsabilités des maîtres des fichiers fixe des obligations à respecter, mais les Directeurs d'hôpital ont toute latitude pour choisir les moyens d'atteindre ces objectifs. Cette autonomie de gestion est une chance parce qu'elle est la possibilité d'une organisation adaptée aux besoins de l'établissement. Elle fait en contrepartie peser une assez lourde responsabilité sur les épaules des dirigeants dans un domaine complexe. Les autorités de tutelle ne contrôlent pas non plus l'opportunité des décisions prises. Elles se contentent de constater la présence ou l'absence d'un schéma directeur des systèmes d'information et ne vérifient pas la qualité de son contenu, qui n'est d'ailleurs pas précisément défini. Aucune obligation en matière de sécurité n'est imposée.

b) Un niveau de sécurité hétérogène dans les établissements

Le GMSIH a publié en mars 2003 une enquête réalisée auprès de ses 400 établissements membres. Parmi ces membres, un échantillon représentatif de 95 questionnaires a été retenu. Ce document dresse l'état des lieux dans les systèmes d'information des établissements de santé.

Les résultats de cette enquête montrent que les établissements de santé paraissent assez mal préparés pour démarrer ou étendre leur politique de sécurité informatique.

- les directions générales semblent encore appréhender de manière incertaine l'importance de la sécurité des systèmes d'information. En particulier, peu d'établissements disposent d'un responsable de la sécurité des systèmes d'information identifié, et parmi ceux qui en disposent, peu ont rédigé une fiche de poste.
- 68% des établissements seulement ont réalisé une analyse des risques informatiques.
- le niveau de sécurité des établissements de santé est inférieur à celui des entreprises privées. Ainsi, 27% des entreprises françaises (et 64% des entreprises de plus de 500 salariés, ce qui est le cas de beaucoup d'hôpitaux) ont mis en place une politique de sécurité, contre seulement 15 % des établissements de santé.

Ces résultats sont peut-être liés au faible degré d'informatisation des établissements et au nombre encore faible des utilisateurs des outils informatiques. Cela révèle sans doute aussi le manque de maturité des politiques de sécurité en santé en général. Une action de sensibilisation doit donc être menée, d'autant plus que seuls 32% des établissements ont mené une telle action auprès du personnel.

Le niveau de sécurité varie sensiblement en fonction de la taille des établissements. Ainsi, alors que 52 % des établissements publics de grande taille (plus de 1000 lits) ont réalisé une analyse des risques, seulement 13% des établissements publics de petite taille (entre 300 et 500 lits) en ont effectué une. La mise en place d'une politique de sécurité informatique est un travail lourd qui demande des compétences particulières, des effectifs relativement conséquents et qui représente un coût financier dont il est difficile de vérifier la rentabilité. Les petites structures, qui présentent une vulnérabilité plus faible, sont donc peu incitées à mettre en place un tel projet.

Dans cet environnement, il s'agit maintenant de déterminer la position du CH de Dreux vis-à-vis des risques informatiques.

1.3 Le Centre hospitalier de Dreux voit son niveau d'exposition aux risques informatiques augmenter

Le CH de Dreux est un des deux EPS de référence du département d'Eure-et-Loir. Il dispose de l'ensemble des services d'un hôpital général, en MCO, soins de suite et de

réadaptation, médecine physique et réadaptation fonctionnelle, santé mentale adultes et infanto-juvénile, long séjour et maison de retraite. Il possède un service d'accueil des urgences et est le siège départemental du SAMU. 761 lits et 43 places y sont installés, ce qui le classe parmi les EPS de taille moyenne. Son évolution en matière d'informatisation a été celle des hôpitaux de taille semblable jusqu'aux années récentes. Peu exposé aux risques jusqu'à présent, il doit maintenant se préoccuper de son degré de vulnérabilité.

1.3.1 L'analyse des risques informatiques au CH de Dreux

A) Les ressources informatiques au CH de Dreux

a) Historique du développement de l'informatique

Les débuts de l'informatisation

Le CH de Dreux a connu une histoire similaire à celle des autres établissements. Les premiers ateliers de mécanographie utilisant la technique des cartes perforées sont apparus en 1961. A l'ouverture de l'hôpital actuel, en 1973, les cartes perforées laissent la place à la technique des bandes magnétiques, plus performante. Le traitement automatisé ne concernait à cette époque que la comptabilité, la gestion des stocks et la paie du personnel. L'hôpital ne disposait pas d'informaticien, le traitement étant effectué par le seul personnel administratif. Ce mode de fonctionnement va perdurer jusqu'à la fin des années 1980, époque à laquelle l'établissement désire disposer d'une informatique autonome. Le ministère de la santé l'incite alors à s'orienter vers la filière proposée aux établissements de sa catégorie : « Symphonie ».

Les années 1988-2004

Le CH de Dreux s'est donc engagé dès 1988 dans la filière « Symphonie ». Les logiciels de cette offre ont été conjointement développés par trois entités publiques : le CHR de Metz pour la partie malade, le CHU de Tours pour la gestion comptable et économique, et le SIR de Poitou-Charentes pour la partie gestion du personnel. L'implication de tous les hôpitaux de cette filière étaient forte et s'exerçaient lors de cercle utilisateurs où la pertinence et les priorités y étaient fixées. Cette filière a permis une informatisation du système de gestion administrative qui répondait aux contraintes de la clientèle et aux exigences de l'hôpital. La filière « Symphonie » qui reste fonctionnellement riche, économe de ressources de toute sorte, a constitué un compromis coût / satisfaction intéressant. Elle a constitué une solution particulièrement appropriée aux besoins exprimés durant la décennie 90 car elle était à la fois complète en ce qui concerne la partie administrative et cohérente par rapport aux besoins d'intégration dans le domaine

médical, médico-technique et de la communication. Les logiciels Symphonie garantissaient une des spécificités primordiales de l'hôpital : son autonomie de gestion budgétaire et financière. Le système d'information couvre également les besoins des secrétariats médicaux qui possèdent le serveur dans leur service. Cette solution, limitée aux secrétariats, est remise en cause par une exigence affirmée des soignants et une sécurisation des données médicales. L'annonce de la fin programmée de la filière « Symphonie » en juillet 2004 a bouleversé les orientations du CH de Dreux, qui avait basé sa politique informatique sur l'exploitation bureautique à l'usage des personnels administratifs et secrétaires médicales.

B) L'organisation matérielle et humaine de l'informatique

a) Les structures de décision et de mise en œuvre de la politique informatique

Le système d'information du CH de Dreux est placé sous la responsabilité d'un directeur adjoint chargé des systèmes d'information et de l'organisation. A l'heure actuelle, cette fonction n'est pas remplie par un Directeur à plein temps, mais est assumée par le Directeur adjoint chargé également des affaires financières, de la clientèle et de la qualité. A l'avenir, il est envisagé de confier cette responsabilité au Directeur adjoint chargé des services économiques et logistiques.

Un Conseil du système d'information hospitalier est constitué. Il comprend vingt et un membres qui se réunissent au moins quatre fois par an, avec une périodicité irrégulière dépendant de l'actualité. Composé de directeurs, d'informaticiens, de cadres infirmiers et surtout de médecins dont son président, les thèmes de réflexion qui y sont abordés tournent essentiellement autour du développement de l'informatique médicale. Cette approche, qui paraît tout à fait légitime dans un EPS, a permis d'envisager la mise en place d'un système d'information « centré patient ».

L'exploitation et le développement du système d'information est confiée à un service informatique. Installé dans des locaux pour l'instant peu adaptés car divisés en deux parties et trop exigus, le service doit bénéficier dans quelques mois d'un espace mieux aménagé et plus spacieux.

b) Un service informatique aux effectifs réduits[16]

Les moyens humains du service informatique sont composés d'un responsable des études informatiques et de cinq informaticiens dont un spécialiste micro, bureautique et assistance de premier niveau, deux spécialistes système, réseau, sécurité et gestion du parc et deux spécialistes dans le suivi des applicatifs et le développement.

Trois de ces informaticiens sont polyvalents. Ils possèdent une double culture qui leur permet de maîtriser aussi bien les logiciels applicatifs que le système.

Ces effectifs sont faibles si on les rapproche des ratios des effectifs de la direction informatique rapportés à l'effectif en personnes physiques de l'établissement établis à l'issue de l'enquête du GMSIH effectuée dans les établissements de santé. Le CH de Dreux fait ainsi partie des 56% des hôpitaux de l'échantillon disposant d'un ratio de personnel informatique inférieur à 5‰, ratio qui correspondrait à un effectif de 8 informaticiens pour un établissement de taille comparable. Les établissements les mieux dotés disposent en proportion d'un effectif deux fois supérieur.

Collaborent cependant au quotidien avec le service informatique des agents administratifs chargés des formations logiciels, des référents pour certaines applications, un cadre infirmier supérieur pour la gestion des plannings et des correspondants dans les différents services (pharmacie, services économiques et logistiques, services financiers…).

c) Les moyens matériels

Le CH de Dreux possède un LAN (Local Area Network), c'est-à-dire un réseau local propre à l'établissement. L'architecture de ce réseau utilisant la technologie Ethernet est organisée en étoile autour d'un routeur qui constitue le cœur de réseau. Ce cœur de réseau est relié à 30 switches (commutateurs) disposés dans l'ensemble de l'établissement. Le réseau est relié par de la fibre optique qui autorise un débit de 100 mégabits par seconde, soit environ 12 millions de caractères par seconde. Les prises informatiques des étages et des bâtiments du site sont reliées à cette ossature du réseau par un câble en cuivre. Ce câblage permet également une sécurité en cas de défaillance des connexions optiques. L'avantage de cette architecture en étoile est de limiter les

[16] Voir annexe II

conséquences d'une panne technique puisque la défaillance d'un switch ne met pas en péril l'ensemble du réseau.

En revanche, ces switches qui sont installés dans différents service de l'hôpital sont ventilés et alimentés, donc bruyants. A l'heure actuelle, le point le plus sensible est le switch situé au cœur du réseau, qui est unique. En cas de défaillance, le réseau tout entier risque de tomber et aucun secours n'est pour l'instant disponible en dehors d'un contrat de maintenance qui permet de garantir une remise en état de marche relativement rapide.

Ce réseau physique est découpé en une dizaine de réseaux virtuels, les VLAN (Virtual Local Area Network). Ce découpage permet d'accroître la sécurité et la confidentialité des données en limitant l'accès de chaque utilisateur à une petite partie de l'ensemble du réseau. Ainsi, le personnel administratif ne peut pas accéder au réseau virtuel réservé aux services de médecine ou au laboratoire par exemple. Seul le service informatique peut avoir une vue d'ensemble du réseau. Ce mode d'administration présente de surcroît l'avantage d'être assez simple à administrer, ce qui permet à l'ensemble des informaticiens d'être capables d'intervenir sur le réseau de l'établissement.

Aujourd'hui, les serveurs ne sont pas centralisés. Il existe un serveur par service, ce qui procure une sécurité relative. D'une part, cela divise le risque de panne, puisque la défaillance d'un serveur ne remet pas en cause l'ensemble du réseau. Mais d'autre part, cela limite la sécurité des informations puisque ces serveurs sont en général placés dans les secrétariats médicaux et sont facilement accessibles.

L'hôpital de Dreux dispose donc au total d'un système d'information cohérent et relativement peu gourmand en ressources humaines et financières, dont la modernisation de l'architecture matérielle a commencé.

1.3.2 Le contexte actuel implique une plus grande maîtrise des risques

A) Le changement de SIH

Le schéma directeur encore en vigueur actuellement a été rédigé fin 1999. Il prévoit le changement du système d'information. En effet, le système d'information actuel est toujours bâti sur la base des applications de l'ex filière Symphonie. Or, en 1999, il a été annoncé que les applications ne seraient maintenues que jusqu'en juillet 2004, laissant donc cinq ans pour faire évoluer le système d'information.

Ce changement de SIH imposé n'est pas sans risque. Une telle opération pose en effet un certain nombre de problèmes. Tout d'abord, le démarrage du système sera un moment délicat. Le choix de la date de basculement d'un système à l'autre présente dans toutes

les hypothèses des difficultés. Certains modules doivent pouvoir être mis en place dès janvier 2004. C'est le cas de la gestion du dossier patient, qui devra tenir compte de l'application de la CCAM. Une contrainte essentielle pour les autres modules est l'arrêt de la maintenance corrective et réglementaire à partir de juillet 2004. Le choix d'un démarrage au 1er janvier 2005 comporterait donc des risques élevés, notamment au moment de la mise en place de la tarification à l'activité. Le basculement devrait donc s'effectuer au 1er juillet 2004. La reprise des données de l'ancien système, avec au moins un historique sur cinq années sera une étape délicate à mener en raison du risque de perte d'informations qui peut en résulter. Le paramétrage des logiciels est également une étape cruciale dans la mise en œuvre du nouveau système. De la qualité de celui-ci dépend la qualité de l'information traitée. Ainsi, le découpage fonctionnel et comptable de l'établissement doit être saisi. Cela comprend, par exemple, le découpage en unités fonctionnelles, en centres de responsabilités, en sections d'analyses, la nomenclature des comptes budgétaires, la répartition des chambres, des lits, etc. Ensuite, les utilisateurs du nouveau système devront être formés à son utilisation afin d'éviter au maximum les erreurs de saisie, les fausses manipulations et la perte de données. Le changement d'interface graphique, l'apparition de nouvelles fonctionnalités vont changer les méthodes de travail et dérouter les utilisateurs pendant quelque temps.

B) L'ouverture croissante du SIH est une évolution qui doit être maîtrisée

a) Le système d'information s'est d'abord ouvert en interne.

La création du réseau intranet et la mise en place d'une messagerie interne ont constitué le premier acte de cette ouverture. Cette première étape présentait un danger limité puisque les utilisateurs du réseau étaient bien identifiés.

b) Le système d'information s'est ensuite ouvert sur l'extérieur avec la possibilité d'accès à Internet.

Dans un premier temps, certains utilisateurs ont pu se connecter par modem. Cette solution transitoire constituait un danger réel d'intrusion et de propagation de codes pernicieux puisque la lutte antivirus reposait sur des logiciels dont la mise à jour coûteuse et contraignante faisait qu'ils étaient rapidement obsolètes, alors que les micro-ordinateurs étaient reliés au reste du réseau local. Dans un second temps, la mise en place d'une connexion à haut débit par ADSL a permis de connecter un grand nombre de postes à un moindre coût et donc de supprimer l'ensemble des modems. L'accès à Internet s'effectue via le fournisseur d'accès OLEANE Santé, qui permet un premier niveau de filtre des entrées sur le réseau local, puisque seuls les professionnels de la

santé ont accès au réseau OLEANE Santé. L'installation d'un mur pare-feu (firewall) est venue renforcer la sécurité du réseau de l'hôpital. Ce dispositif matériel et logiciel permet de restreindre en un seul point l'entrée sur le réseau de l'hôpital et filtre les communications, détecte les virus au moyen d'un logiciel mis à jour automatiquement et peut crypter l'information.

c) Les réseaux de santé ville-hôpital et hôpital-hôpital sont encore quasiment inexistants.

Seule la maternité est reliée à un réseau « périnatalité en pays drouais » accessible via une connexion Internet. Ce réseau présente un inconvénient car il s'est mis en place sans qu'une étude préalable ait été menée par le service informatique. Le faible volume d'informations échangées au sein d'une communauté de professionnels identifiés restreint cependant le niveau de risque.

C) L'utilisation des technologies nomades va augmenter le niveau de risque

Un essai de mise en place d'un réseau local sans fil est en cours d'étude aux urgences. La nomadisation constitue en effet un atout incontestable pour les professionnels de santé qui ont ainsi la possibilité de disposer au chevet du patient de l'ensemble des informations nécessaires à son traitement.

a) Les avantages de la technologie sans fil

Ce type de réseau permet de remplacer une ou plusieurs liaisons matérielles de transmission de données par des ondes radio-électriques. Le standard dominant aujourd'hui est la technologie Wi-Fi[17], apparue en 1997.

Cette technique présente quelques avantages, dont le remplacement à moindre frais du câblage de tout ou partie d'un bâtiment, le raccordement rapide d'équipements sans les démarches et les délais d'extension d'un réseau existant et l'accès aisé au réseau de l'établissement d'équipements nomades (ordinateurs portables, PDAs, qui par nature n'aiment pas les fils). Un des gros avantages de la technologie Wi-Fi est également sa facilité de déploiement, puisqu'il suffit d'une prise de courant et d'un accès réseau.

b) Les inconvénients de cette technologie

Cette technologie présente cependant quelques inconvénients qui sont le prix à payer pour sa souplesse d'utilisation. Comme toute émission radio, celle des réseaux sans fils

[17] Wireless Fidelity

se propage dans un volume centré sur l'antenne d'émission et peut donc être captée par tout autre récepteur placé dans ce volume. Concrètement, on peut imaginer qu'un patient disposant d'un ordinateur portable équipé puisse capter les données échangées sur le réseau de l'hôpital si les précautions nécessaires ne sont pas prises. De plus, la portée dépasse plus ou moins largement le bâtiment dans lequel se trouve l'antenne d'émission. Ainsi, l'utilisation d'antennes directionnelles disponibles dans le commerce ou pouvant être fabriquées soi-même peut décupler sa zone de couverture, rendant le réseau accessible depuis l'enceinte de l'hôpital, voire les habitations avoisinantes[18]. La dernière version du standard Wi-Fi rend cette fraude plus difficile car elle intègre un mécanisme simple de chiffrement des données[19].

c) La vulnérabilité des technologies nomades

Un autre inconvénient des technologies nomades est leur vulnérabilité au vol, leur moindre fiabilité et la multiplication des risques de chute. Ainsi, il est indispensable de protéger les ordinateurs portables de ces dangers et d'envisager des dispositifs simples comme leur fixation sur des chariots.

1.3.3 Les menaces potentielles et la sinistralité recensée au CH de Dreux

La typologie des risques qui pèsent sur le SIH est très complexe[20]. Toutefois, il est possible de classer les menaces dans trois catégories : les accidents, les erreurs et les malveillances.

Le panorama ci-dessous ne prend en compte que les incidents significatifs. Les informaticiens sont en effet régulièrement appelés pour effectuer une maintenance de routine consistant généralement à remettre en marche un ordinateur ou un périphérique bloqué, ou à aider à la récupération d'une erreur de manipulation sans gravité. De manière générale, la sinistralité recensée au CH de Dreux est quantitativement faible mais certains incidents méritent d'être pris en compte car ils auraient pu avoir des conséquences sur la santé des malades.

A) Les accidents

Les accidents peuvent correspondre à une destruction partielle ou totale, ou à une dysfonction des matériels, des logiciels et de l'environnement technique dans lequel est mis en œuvre le système d'information.

---

[18] Cette pratique est appelée « war-driving » ou « war-Xing »
[19] Il s'agit du WEP (Wired equivalent privacy »
[20] Voir une représentation graphique de cette typologie en Annexe I

a) La destruction peut avoir des origines très variées.

Hormis les catastrophes majeures comme l'incendie ou l'inondation, les machines peuvent être exposées à des chocs ou à des chutes, au déversement de liquides, souvent alimentaires tels que le café, à des contacts physiques avec des sources de chaleur, à des expositions solaires importantes, à l'existence de champs électromagnétiques intenses, à l'arrachage des câbles de connexion. Absolument tout, même le plus absurde, peut se produire, parfois en raison de hasards malencontreux et imprévisibles, mais bien le plus souvent en raison de l'inconscience des utilisateurs.

Au CH de Dreux, La récente vague de chaleur a permis de révéler l'insuffisante maintenance du système de climatisation du local technique, dont le moteur plein de poussière n'avait pas été nettoyé depuis deux ans. La qualité de l'air ambiant d'une salle d'ordinateurs est un paramètre essentiel, contribuant au bon fonctionnement des machines et permettant d'obtenir un rendement optimum. Les constructeurs recommandent généralement pour des machines en fonctionnement une température de l'air de 20°C avec plus ou moins 2°C d'écart. Or, la température à l'intérieur du local est montée jusqu'à 36°C. Un serveur disposant d'une procédure de protection contre la surchauffe s'est arrêté au-delà de 30°C afin d'éviter l'altération de ses composants qui supportent mal les variations de température et surtout les températures extrêmes.

b) Les dysfonctionnements des matériels et des logiciels

Ces dysfonctionnements sont également à prendre en compte, même si leur survenue est généralement imprévisible. Ils peuvent être liés à la carence ou à la défaillance des équipements telle une panne dans le circuit d'alimentation électrique.

Une panne d'alimentation électrique a, en juin 2003, privé l'établissement d'électricité pendant une vingtaine de minutes. L'essai de groupe électrogène mensuel combiné avec une coupure d'alimentation sur un transformateur en vue d'une intervention technique a été à l'origine de cet incident. L'onduleur qui devait, selon l'avis du fournisseur, se mettre en marche automatiquement a dans les faits du être enclenché manuellement. Là encore, cet incident qui a eu lieu à 7H30 n'a eu aucune conséquence pour l'établissement.

En 2001, le serveur du SAMU a connu une panne d'origine technique qui a privé le personnel de l'utilisation de la base de données qu'il stockait.

c) La défection des personnels techniques chargés de la manipulation du système ou de sa maintenance.

Cet autre type d'événement préjudiciable, rarement cité n'en constitue pas un des moindres. Il peut s'agir d'un arrêt maladie ou d'un départ sans préavis de la secrétaire, de l'indisponibilité du prestataire informatique par exemple…

B) Les erreurs

L'analyse des accidents dans les systèmes complexes impute 65 à 80% des causes immédiates aux opérateurs de première ligne dans l'industrie et les transports publics[21]. James Reason explique que l'homme recherche la performance et est amené à prendre des risques dans toutes ses activités. En conséquence, les erreurs sont fréquentes dans les activités humaines, même si leur taux de détection et de récupération par leur auteur est importante, de l'ordre de 80%[22].

En matière informatique, les erreurs peuvent survenir lors de la saisie des informations, de leur transmission par le système d'information, de la manipulation de ses fonctions d'exploitation, ou résulter de sa mauvaise utilisation.

Fin 1999, en prévision du passage à l'an 2000, des tests de sauvegarde sont effectués. Parce qu'une partie d'un fichier de la base patients des urgences avait été déplacé, la restauration de la sauvegarde s'avérera incomplète, privant le service des urgences de six mois de données.

a) L'erreur de saisie

L'erreur de saisie la plus redoutable lors de l'utilisation d'un système est l'indexation insuffisante qui empêche le regroupement des données fournies à des fins diagnostiques et thérapeutiques sous l'identité du patient concerné. Une erreur de manipulation dans les documents papier initiaux attribuera par exemple les signes cliniques d'un patient à un autre patient, ce qui n'est pas forcément anodin. Ces risques d'erreur sont limités lorsque le système est utilisé en temps réel mais leur probabilité croît dès qu'il fonctionne en temps différé. D'autres erreurs peuvent également survenir lors de la saisie des éléments cliniques des dossiers des patients, spécialement lorsqu'ils sont codés comme dans le

[21] HOLLNAGEL E. Human reliability analysis. Context and control. London : Academic Press, 1993

[22] REASON J. *L'erreur humaine*. Paris : Presses universitaires de France, 1993

PMSI. Leurs conséquences varieront en fonction de la nature de l'erreur et de l'utilisation qui est faite de l'information. Les erreurs de manipulation prennent aussi des formes variées : absence de saisie d'un document, écrasement des données avant sauvegarde, destruction des archives…

b) L'altération de la qualité des informations

Quand il y a transmission de l'information, la gravité des erreurs peut être liée à la nature des réseaux utilisés et du type de données transmises. Si une perte de quelques bits d'information peut n'altérer que faiblement la qualité d'un transfert d'images, elle peut modifier fondamentalement la signification d'un résultat chiffré.

De même une altération de la définition des images transmises est pratiquement sans conséquence sur l'examen macroscopique d'une pièce anatomique par exemple, alors qu'elle peut rendre impossible l'analyse d'une image microscopique ou constituer un artefact important.

c) Les erreurs de conception

Les erreurs de conception d'un système d'information sont théoriquement rares si son adéquation au service a été bien testée par les utilisateurs et les informaticiens. Cependant, les contraintes induites par les conditions d'environnement rencontrées en pratique quotidienne peuvent avoir été sous estimées. Une utilisation trop intense peut entraîner un dépassement des capacités de traitement du microprocesseur, une saturation des mémoires ou du réseau de transmission des informations. De même, certains éléments du système relativement délicats, comme un scanner de lecture, peuvent ne pas supporter des manipulations trop rapides ou trop fréquentes et nécessiter de fréquents renouvellements. Dans cette catégorie d'erreurs de conception, on doit signaler qu'une bonne ergonomie des postes et stations de travail est indispensable pour réduire la fatigue des personnels travaillant sur écran.

C) La malveillance

a) Le vol de matériel

Dans un système d'information, les trois éléments principaux, le processeur, le moniteur et les périphériques d'impression et de saisie sont des éléments susceptibles d'intéresser beaucoup de monde. Les personnes à l'origine de ces vols peuvent venir d'horizons divers : personnels, patients, visiteurs… Un moment d'inattention peut rapidement permettre la disparition d'une partie importante du matériel.

Le vol de matériel est un fléau commun à l'ensemble des entreprises. Comme le matériel informatique est encore relativement onéreux, les motivations financières sont souvent supérieures à l'intérêt des données contenues sur les disques des ordinateurs. Ce type de malveillance n'en porte pas moins atteinte à la confidentialité des données.

En 2000, trois serveurs installés à la maternité ont été dérobés. Plus récemment, en mai 2003, un micro-ordinateur a été volé au Centre médico-psychologique.

b) Le détournement de biens immatériels

Dans un système d'information, il correspond à la copie des fichiers de données ou des logiciels de gestion du système. La première conduit essentiellement à un viol de la confidentialité et la seconde à une atteinte à la propriété intellectuelle ou industrielle. Ces détournements s'effectuent sur place ou par l'intermédiaire du réseau existant.

c) L'altération des biens immatériels

Elle correspond soit à la destruction physique directe de tout ou partie de l'ensemble des fichiers et des logiciels comme de leurs sauvegardes, ou à leur destruction indirecte par l'intermédiaire d'instructions informatiques introduites dans les logiciels telles que virus, bombes logiques, « vers », ou encore par des usurpations d'identité donnant accès aux fonctions d'exploitation du système informatique. En cas d'échanges interactifs avec l'extérieur, un système d'information s'expose aux intrusions et aux usurpations d'identité.

Les virus et autres codes pernicieux constituent néanmoins un risque fréquent, même s'il est l'un des mieux maîtrisés. Des virus ou vers sont ainsi régulièrement détectés par le logiciel antivirus. La protection de haut niveau mise en place depuis un an a permis d'éviter de subir les conséquences de ces attaques virales. En revanche, lorsque les connexions par modem existaient encore, des stations de travail ont du être réinstallées suite à une infection.

Le sabotage est en revanche plus rare et le plus souvent d'origine interne. Aucun cas n'a été recensé à Dreux.

Au terme de cette partie de l'étude, il apparaît que si les risques avérés en l'état actuel du système d'information du CH de Dreux étaient encore faibles il y a un an, les risques nouveaux et potentiels engendrés par le changement de progiciel et l'ouverture du réseau local sur l'extérieur sont à prendre en compte. La culture hospitalière étant fondée sur l'ouverture au monde extérieur ainsi que sur l'obligation éthique et déontologique de mettre toutes les technologies disponibles en œuvre pour soigner les malades, l'investissement humain et financier dans une politique de protection contre les risques

liés à l'informatique ne peut être compris que si les enjeux sont bien identifiés et peuvent susciter l'adhésion des professionnels de santé.

2 LES ENJEUX DE LA SECURISATION DU SYSTEME D'INFORMATION HOSPITALIER

Les enjeux les plus palpables de la sécurisation du SIH sont d'ordre juridique. En effet, la législation relative à la protection des droits des citoyens vis-à-vis des traitements automatisés des données est très développée et même renforcée en ce qui concerne les données médicales. L'attention du Directeur d'hôpital doit donc être retenue quant aux risques juridiques encourus par lui-même comme par l'établissement en cas de non-respect de cette réglementation. Ce risque juridique peut alors se transformer en risque économique que des démarches d'amélioration de la qualité et de gestion des risques peuvent permettre d'éviter.

2.1 Pour les établissements, les enjeux juridiques d'une gestion des risques informatiques sont forts

La législation est foisonnante en termes de droits des patients et d'obligations pour les responsables des fichiers informatisés. Les tribunaux trouvent là des bases pour mettre en œuvre la responsabilité des établissements et de leurs dirigeants.

2.1.1 Les droits des patients sont bien protégés

A la fin des années 1960, apparaissent les premières inquiétudes sur les capacités de la grosse informatique centralisée, surtout celle de l'administration publique, de porter atteinte aux droits et libertés fondamentaux des personnes. On peut parler à l'époque de la peur de Big Brother. De nombreuses réflexions mènent alors à des textes législatifs protecteurs spécifiques.

A) Les sources principales du droit

a) Normes internationales

La Convention de sauvegarde des droits de l'homme et des libertés fondamentales a été signée à Rome en 1950 dans le cadre du Conseil de l'Europe. Son originalité et son importance proviennent de l'institutionnalisation de deux organismes capables de protéger les droits et libertés, la Commission européenne des droits de l'homme et la Cour européenne des droits de l'homme. Depuis 1981, les citoyens français peuvent saisir directement la Cour. Cette dernière a développé une jurisprudence riche et importante. Dans un arrêt MS c/Suède du 27 août 1997, elle « rappelle que la protection des données à caractère personnel revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale ».

La Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel du 28 janvier 1981 (convention 108) a largement inspiré les rédacteurs de la directive communautaire du 24 octobre 1995 et est largement compatible avec la loi de 1978. Elle est le premier instrument international juridiquement contraignant sur le sujet et puise sa source directement dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales de 1950. Elle a une vocation universelle puisqu'elle est ouverte à l'adhésion de tous les pays membres du Conseil de l'Europe et aux pays non membres. Elle a pour but de « garantir […] le respect des droits et des libertés fondamentales et notamment de la vie privée à l'égard du traitement automatisé de données à caractère personnel ». Elle établit des principes de base sur la qualité des données, le droit d'accès et de rectification ou d'effacement des données, protège la sécurité des données et spécialement celle des données sensibles. L'intégration de la Convention 108 dans le droit français a été reconnue à plusieurs reprises par le Conseil d'Etat ; aussi faut-il considérer que ses dispositions principales sont d'applicabilité directe, ce qui permet de s'en prévaloir dans le droit français. De manière systématique, la CNIL vise la convention.

b) Les normes communautaires

L'article 6, second alinéa du traité sur l'Union européenne dispose « l'Union respecte les droits fondamentaux tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, […] et tels qu'ils résultent des traditions constitutionnelles communes aux Etats membres, en tant que principes généraux du droit communautaire ». Par ces renvois, la protection des données informatisées se trouve déjà garantie. Des textes propres à l'Union européenne sont de plus venus renforcer ces garanties.

La Charte des droits fondamentaux de Nice de 2000 a été reprise dans le projet de constitution de l'Union européenne dont l'article II-8 est intitulé « protection des données à caractère personnel ». Il dispose que « 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.»

Afin de définir une exigence de protection commune à l'ensemble des pays de l'Union européenne, est née la directive du 24 octobre 1995, approuvée par une décision conjointe du Parlement européen et du Conseil des ministres. La transposition de cette directive doit être l'occasion d'une modernisation de la loi du 6 janvier 1978. Toujours en

cours, elle a connu une première étape législative avec un premier vote de l'Assemblée nationale le 30 janvier 2002. Conformément à la jurisprudence de la Cour de justice des communautés européennes, reprise en partie par le Conseil d'Etat, les particuliers peuvent invoquer une directive non ou mal transposée à l'encontre de l'Etat, mais pas à l'encontre d'un autre particulier. Le Conseil d'Etat a définit les conditions de cet effet direct[23].

c) Les normes nationales

La loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés a été suscitée par des événements touchant pour certains le domaine de la santé publique et perçus comme des menaces pour les libertés : projet de gros système centralisé pour la gestion de la santé et des hôpitaux, projet GAMIN [24] de protection infantile notamment. La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est encore actuellement le texte de base en matière de protection des données personnelles. L'article 1er de cette loi pose que « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. ». La plupart des droits et libertés protégés par cette loi se voient attribuer une valeur constitutionnelle par le Conseil constitutionnel, ce qui situe la loi de 1978 au plus haut niveau. Il en va ainsi de la liberté des personnes, protégée par la Déclaration des droits de l'homme et du citoyen de 1789, et consacrée par l'article 66 de la Constitution de 1958. Défenseur de la liberté individuelle, le Conseil constitutionnel devient le protecteur de la loi informatique, fichiers et libertés. Le droit à la vie privée s'est également vu attribuer une valeur constitutionnelle par le Conseil constitutionnel[25]. La législation «informatique et liberté» protège également les libertés publiques, ce qui comprend en particulier les libertés de pensée, de conscience et de religion, d'opinion, de communication, etc. Le Conseil constitutionnel oblige le législateur à intervenir en la matière de manière suffisamment préventive, précise et détaillée pour rendre plus effectif l'exercice des droits et libertés fondamentaux et interdit tout retour en arrière amoindrissant ou supprimant le niveau de protection atteint.

B) Les droits de s'informer et d'accéder aux données personnelles

Ils concernent non seulement les patients mais aussi le personnel de l'établissement.

---

[23] CE 22 décembre 1978, *Cohn-Bendit* ; CE 6 février 1998, *Tête et association de sauvegarde de l'Ouest lyonnais*

[24] Gestion automatisée en médecine infantile

a) La finalité du traitement

Les fichiers des établissements de santé, comme tous les fichiers du « secteur public », sont autorisés par un acte réglementaire pris après avis motivé de la CNIL. Il est à noter que la Directive européenne 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, non encore transposée en droit français, prévoit une harmonisation des régimes : il n'y aura plus de distinction entre les fichiers du secteur public et ceux du secteur privé. Dans tous les cas, une notification (déclaration) sera à effectuer auprès de l'autorité compétente (CNIL). Pour les catégories de traitements qui ne comportent pas d'atteinte manifeste à la vie privée et aux libertés, une déclaration simplifiée à déposer auprès de la CNIL suffit. Il est à noter que l'article 19 du décret du 17 juillet 1978 dispose que « dans le cas de traitements automatisés opérés pour le compte d'un établissement public […] la décision est prise par l'organe délibérant chargé de leur administration ». Dans le cas de l'hôpital, il s'agit donc de son Conseil d'administration, et non de son Directeur. Le non-respect de cette procédure a conduit certains hôpitaux à voire leur décision annulée car entachée d'incompétence.[26]

Tout intéressé doit être informé, sous réserve d'opposition de sa part, de toute opération de collecte, de gestion, de traitement, de communication le concernant. En outre, pour les données de santé, tout intéressé doit donner son autorisation au maître du fichier.

Toute personne prise en charge par un professionnel, un établissement ou un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et au secret des informations le concernant. Deux ou plusieurs professionnels de santé peuvent, 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.

Les informations nominatives ne peuvent être collectées et traitées que pour des finalités déterminées et légitimes. De même, elles ne peuvent être conservées que pour la durée nécessaire à la réalisation de ces finalités.

---

[25] Décision n°99-416 DC du 23 juillet 1999, Couverture maladie universelle

[26] Par exemple, CE 15 décembre 2000, *Syndicat national de défense de l'exercice libéral de la médecine*

b) Le droit à l'information

Les personnes auprès desquelles sont recueillies les données doivent être informées du caractère obligatoire ou facultatif des réponses, des conséquences d'un défaut de réponse, des destinataires des informations et de lexistence d'un droit d'accès et de rectification, ainsi que de l'identité du maître du fichier et des finalités du traitement. La forme que doit revêtir l'information ne fait l'objet d'aucune disposition spécifique. En pratique, au CH de Dreux un paragraphe du livret d'accueil et une affichette accrochée au bureau des admissions et dans les services avertissent les patients de l'existence d'un système d'information automatisé dans l'établissement.

c) Le droit d'accès

Le droit d'accès donne à toute personne la possibilité de connaître l'existence ou non de données la concernant dans un fichier et, si elle le désire, d'en obtenir communication. Toute personne a accès à l'ensemble des informations concernant sa santé détenues par des professionnels des établissements de santé qui sont formalisées et ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention, ou ont fait l'objet d'échanges écrits entre professionnels de santé, notamment les résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et des prescriptions thérapeutiques mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé, à l'exception des informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant un tel tiers. Lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de l'article L.1111-7 du CSP. Plus précisément, les établissements 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. Concernant les données médicales nominatives des patients et dans les cas où la loi impose ou autorise leur transmission à des organismes tiers, les professionnels de santé doivent en informer leurs patients de façon à ce qu'ils puissent exercer les droits qui leur sont reconnus par la loi du 6 janvier 1978. Ainsi, hors les cas où la transmission est imposée par la loi, les patients doivent pouvoir s'opposer aux communications d'informations les concernant.

L'accès direct au dossier médical fait l'objet de nombreuses demandes depuis la mise en application de la loi du 4 mars 2002. En revanche, l'accès aux données informatisées n'a

jamais fait l'objet d'une demande de la part des patients. En ce qui concerne le personnel, après un rappel de ses droits par une note de service du Directeur, seuls deux agents ont demandé à avoir accès aux données contenues dans leur dossier administratif. Ces demandes n'ont pas entraîné l'exercice des doits de contestation ou de rectification.

C) Les droits de contestation et de rectification des données personnelles, le droit d'opposition

a) Le droit de contestation

L'exercice du droit d'accès permet à la personne d'obtenir communication des données personnelles la concernant. Elle peut s'en tenir là. Mais la personne, en application de la législation informatique et libertés se voit offrir au surplus le droit de contester auprès du responsable du traitement la qualité et le sens des informations pour obtenir une éventuelle rectification ou même un effacement ou un verrouillage. Ce droit est d'un usage ouvert, libre et peut être exercé à tout moment.

b) Le droit de rectification

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. En cas de contestation, la charge de la preuve est renversée et « elle incombe au service auprès duquel est exercé le droit d'accès ». L'application de ce droit en matière médicale suscite évidemment des difficultés liées à des demandes plus ou moins motivées et qui risquent de porter préjudice au patient. Ce droit comporte aussi le « droit à l'oubli », c'est-à-dire le droit de voire supprimées des informations périmées, ce qui s'oppose à la réglementation des archives médicales qui impose des délais de conservation très importants, soixante-dix ans pour beaucoup d'entre eux.

c) Le droit d'opposition

L'article 26 de la loi du 6 janvier 1978 dispose que toute personne a la possibilité de s'opposer « pour des raisons légitimes » à figurer dans certains fichiers ou de refuser la communication des informations qui la concernent à des tiers. Il existe différentes formes d'expression de ce droit d'opposition : le refus de répondre lors de la collecte non-obligatoire de données d'une part, et la possibilité d'exiger la non-communication des informations d'autre part. Toutefois, une exception est prévue pour les patients admis

dans les hôpitaux publics. La CNIL est revenue sur cette disposition en 1992[27] en affirmant que « le droit d'opposition s'applique dans tous les cas, sauf mention contraire expressément portée dans l'acte réglementaire créant le traitement ». Cette interprétation est sujette à controverse et source d'incertitude juridique. En cas de litige entre un EPS et un patient sur ce point, l'affaire pourrait être portée devant le tribunal administratif dont on ne sait pas quelle solution il adopterait. L'exercice de ce droit à l'hôpital pose néanmoins problème puisque la loi ne prévoit pas la procédure selon laquelle doit être menée l'opposition ni quelles peuvent être les « raisons légitimes ». En l'absence de précision, là encore, le juge administratif pourrait être amené à trancher. Il semble heureusement que l'exercice de ce droit soit extrêmement rare.

2.1.2 Le responsable du traitement de données a des obligations

Pour protéger les droits et libertés des personnes, il ne suffit pas que la personne concernée par les données dispose de droits personnels leur permettant, à condition d'avoir une attitude active, d'exercer un contrôle sur les données traitées. Il faut aussi en amont que le responsable du traitement, de manière préventive, limite ou empêche la survenance des risques attachés à la gestion des données qu'il traite en appliquant et en respectant des principes établis par la législation. Ces principes établis par la loi ont aussi pour fonction de protéger, d'une certaine manière, le responsable du traitement. Il dispose en effet d'un cadre juridique clair, sécurisant, explicite, à l'intérieur duquel il peut créer et développer son traitement dans le respect de la légalité, dans un climat de confiance vis-à-vis des personnes concernées par les données.

A) L'obligation de respect des principes relatifs à la qualité des données

a) Le secret médical et le secret professionnel dans les textes législatifs et réglementaires

La connaissance de l'état de santé d'une personne constitue une information qui relève de l'intimité de sa vie privée et qui est protégée par le secret médical. Le secret professionnel couvre toute information portée à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire ce qui lui a été confié, ce qu'il a vu, entendu ou compris. Excepté dans les cas de dérogation expressément prévus par la loi, le secret professionnel couvre l'ensemble des informations concernant la personne prise en charge venues 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

[27] CNIL, *13e rapport d'activité*, 1992

personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous professionnels intervenant dans le système de santé.

b) Les limites au secret médical : la communication nécessaire des informations médicales

Toutefois, la CNIL préconise que les transmissions autorisées de données nominatives éventuellement effectuées entre professionnels de santé soient réalisées dans des conditions garantissant de façon effective la confidentialité des données, et qu'en particulier il puisse être recouru à leur chiffrement dans le cadre de la réglementation française et européenne en vigueur. De plus, les autorités judiciaires sont autorisées, lorsqu'elles agissent en flagrant délit ou sur commission rogatoire, à obtenir communication d'informations issues de fichiers sans que les professionnels de santé ne puissent s'y opposer. Les professionnels de santé peuvent également transmettre à des fins statistiques, des données médicales nominatives issues de leur activité à des organismes autorisés à mettre en œuvre, à des fins de recherche médicale, des traitements de données de santé à caractère personnel. De la même manière, les professionnels de santé peuvent transmettre les données nominatives qu'ils détiennent dans le cadre d'un traitement ayant pour fin la recherche médicale.

c) Les dispositions pénales : l'obligation de sécurité matérielle des dossiers, les délits de divulgation et de détournement

La révélation d'informations à caractère secret par une personne qui en est dépositaire, soit par état, soit par profession, hormis les cas où la loi l'impose ou l'autorise, est passible d'un an d'emprisonnement et de 15 000 euros d'amende[28]. Le fait d'obtenir ou de tenter d'obtenir la communication des informations de santé du patient pris en charge en violation de cet article est puni des mêmes peines.

B) L'obligation de respecter le droit au consentement

a) Le droit au consentement

La Directive européenne du 24 octobre 1995 classe les données relatives à la santé parmi les données sensibles, de sorte que le consentement préalable de l'intéressé à la mise en place du fichier est requis. La CNIL recommande que les instances ordinales

[28] Article 226-13 du Code pénal

soient consultées lors de la mis en place de fichiers d'informations médicales, en particulier sur les modalités de participation des professionnels de santé.

b) Les dérogations à l'obligation de respecter le droit au consentement

Toutefois, ce consentement n'est pas requis si le traitement des données est nécessaire aux fins de la médecine préventive, de diagnostics médicaux, de l'administration de soins ou te traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis à une obligation de secret. De même, si le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.

C) L'obligation de respecter le droit à la sécurité des données

Cette obligation figure dans la loi du 6 janvier 1978 et est reprise dans la directive du 24 octobre 1995. Pour y satisfaire, il faut assurer la confidentialité, l'intégrité et la disponibilité des données.

a) Mise en œuvre de cette obligation

Il incombe au maître du fichier de prendre toutes les précautions nécessaires pour préserver la sécurité des informations collectées et pour empêcher leur divulgation et leur déformation. Est mis à la charge du maître du fichier une obligation de précaution afin de préserver la sécurité des données et notamment d'empêcher leur altération ou encore leur divulgation à des tiers. Cette disposition a vocation à s'appliquer à l'ensemble des responsables de traitements d'informations nominatives, sans distinction du secteur dans lequel ce traitement intervient. La CNIL indique qu'il appartient au maître du fichier nominatif de prendre, sous sa responsabilité, les mesures générales de sécurité nécessaires, quelle que soit la puissance du système intéressé, concernant notamment :

- le contrôle de la fiabilité des matériels et des logiciels qui doivent faire l'objet d'une étude attentive afin que des erreurs, lacunes et cas particuliers ne puissent conduire à des résultats préjudiciables aux personnes.
- 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.

b) Recommandations de la CNIL relatives aux données partagées en réseau

Enfin, la CNIL a mené une réflexion approfondie s'agissant du domaine de la santé. Sur ce point, la CNIL énonce des recommandations minimales sur les mesures de sécurité à

adopter pour les applications de données médicales fonctionnant en réseau (rapport de la CNIL de mars 1999). Ces recommandations portent sur :

- les modalités d'authentification des utilisateurs (gestion des mots de passe, modalités de connexion et de déconnexion).
- sur la confidentialité des données. Elle préconise l'utilisation du codage des données nominatives, le cryptage, la mise en place de firewalls en cas de connexion à un réseau ouvert de type Internet.
- l'intégrité des données. La CNIL recommande la mise en place de protocoles de transmission adaptés permettant de vérifier la conformité des données reçues à celles émises, l'utilisation de procédés garantissant l'intégrité de l'image en cas de numérisation et de compression de l'image.

La directive communautaire du 24 octobre 1995 met à la charge du maître du fichier une présomption de responsabilité qui vise tout dommage du fait d'un traitement illicite et ne prévoit l'exonération du responsable de fichier que s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

2.2 Le non-respect de ces droits et de ces obligations risque d'entraîner la mise en oeuvre de la responsabilité juridique de l'établissement et des professionnels

2.2.1 La notion de risque a fait évoluer le droit de la responsabilité

A) Le risque était à l'origine situé hors du droit de la responsabilité

a) Du Moyen-Age au XIX^e^ siècle : le risque considéré comme « coup du sort »

Pendant longtemps, le risque est demeuré aux marges du droit. Les juristes ne le considéraient qu'en lui reconnaissant le statut de «coup du sort », du destin. Le mot, jusqu'au début du XIX^e^ siècle, ne désigne d'ailleurs que des événements dommageables de la nature, à l'exclusion des dommages qui pourraient provenir du fait de l'homme.

b) Le risque est alors destructeur du rapport juridique

Le risque exonère celui qui pourrait apparaître comme le responsable du dommage. Il prend donc la forme de la force majeure.

c) En conséquence, il n'existe alors pas de prise en charge organisée du risque et des dommages associés

Il est tout au plus possible d'envisager que la charité se manifeste au profit de la victime, ou que se mettent en place quelques solidarités familiales ou de proximité. Il n'est pas concevable d'organiser socialement et juridiquement une prise en charge du risque et des dommages associés.

B) Le risque fondement de la responsabilité

a) Une nouvelle approche du risque avec la multiplication des dommages liés à la Révolution industrielle

Ce n'est qu'avec l'essor de la société industrielle et avec la multiplication des dommages que va naître puis se développer une autre approche du risque. Celle-ci sera à l'origine d'un véritable bouleversement de la responsabilité juridique et tout spécialement de la responsabilité civile. A côté de l'événement naturel catastrophique et imprévisible qui demeure un fait exonératoire, il faut prendre en considération l'organisation sociale, l'organisation de l'entreprise, l'introduction et l'utilisation de nouvelles technologies, qui sont facteurs de risques et de dommages qu'il n'est plus possible de laisser à la charge des seules victimes. Ainsi, le risque devient fondement de la responsabilité.

b) La rupture du lien entre responsabilité juridique et faute entraîne un droit à réparation

Ainsi, le lien entre la responsabilité juridique et la culpabilité est pour la première fois rompu. L'homme est tenu de réparer le dommage non parce qu'il a commis une faute mais parce que son activité est génératrice de risques dont certains se réalisent en entraînant des dommages. Ce progrès social est rendu possible grâce à la mise en place de mécanismes d'assurance.

c) La responsabilité pénale change avec l'apparition des infractions matérielles : asymétries d'information

La responsabilité pénale elle-même est affectée par ce mouvement. D'une part, apparaissent des infractions matérielles, c'est-à-dire qui n'exigent pas la preuve d'un élément intentionnel. D'autre part, les victimes prises en charge de manière globalement satisfaisantes sur le terrain de la réparation des dommages éprouvent une sorte de frustration à ne plus identifier ceux qui sont à l'origine du dommage. Elles tentent alors de compenser ce manque en engageant des poursuites pénales.

C) L'apparition du principe de précaution fait évoluer le droit de la responsabilité

a) Un concept qui vient du droit anglo-saxon introduit par le biais du droit international.

Le droit anglo-saxon visait depuis de longues années de plus en plus souvent la négligence. Dans la mise en œuvre du principe de précaution, la faute n'est pas d'avoir agi ou de s'être abstenu d'agir, elle est de n'avoir pas mis en place les procédures qui permettaient de produire de la connaissance sur un risque potentiel mais non encore avéré.

b) La réintroduction de la faute dans le droit des risques

Il s'agit en quelque sorte d'une réintroduction de la responsabilité pour faute considérablement élargie.

c) Une responsabilité pour faute élargie mais encadrée

L'obligation de précaution naît lorsqu'il existe un « doute légitime », ce qui peut se produire dans deux hypothèses. D'une part, lorsque des faits objectifs, c'est-à-dire établis de manière rigoureuse, font naître des questions qui ne reçoivent de réponse que sous la forme d'un doute. D'autre part, lorsque des faits sociaux mesurables révèlent l'existence d'une perception sociale du risque. L'existence de tels doutes imposent alors une obligation de précaution, c'est-à-dire la mise en place de procédures d'expertise, de débats, de procédures de veille et de suivi.

2.2.2 La mise en oeuvre de la responsabilité réparatrice

A) Principe

L'article 11 de la loi du 13 juillet 1983 dispose que «les fonctionnaires bénéficient, à l'occasion de leurs fonctions, d'une protection organisée par la collectivité publique dont ils dépendent (…) » et que « la collectivité publique doit, dans la mesure où une faute personnelle détachable de l'exercice de ses fonctions n'est pas imputable à ce fonctionnaire, le couvrir des condamnations civiles prononcées contre lui… ». Cet article consacre l'intégration au statut de la fonction publique d'une distinction opérée par le Tribunal des conflits en 1875. Les fautes du fonctionnaire, et particulièrement du directeur d'hôpital, sont rarement détachables du service. Sa responsabilité n'est donc qu'exceptionnellement engagée pour ce genre de motifs. Une de ses obligations de service exige en revanche qu'il assure l'organisation et le bon fonctionnement de l'hôpital, afin que la responsabilité administrative ou pénale de l'établissement ne soit pas mise en cause. Les cas d'engagement de la responsabilité du directeur d'hôpital sur le terrain de

la faute de service sont donc nettement plus fréquents. L'organisation et le fonctionnement du service public hospitalier ne présentent pas de difficulté particulière aux yeux du juge administratif. En conséquence, la jurisprudence reconnaît depuis longtemps qu'une simple faute suffit pour engager la responsabilité du service à ce titre. Il est de la responsabilité du directeur d'établissement de mettre en œuvre une politique de gestion des risques qui permette de limiter les cas de mise en cause du service public hospitalier.

C'est en effet l'hôpital qui est mis en cause lorsque, par exemple, la non disponibilité du système d'information est à l'origine d'un dommage. Or, il appartient au directeur de s'assurer de l'absence de dysfonctionnement. Sa responsabilité est donc engagée en tant que représentant légal de l'établissement. La procédure aboutit concrètement à la condamnation de l'hôpital, qui se substitue au directeur coupable de la faute de service, à verser des indemnités aux éventuelles victimes.

B) La mise en œuvre de la responsabilité civile

a) Faute personnelle

L'arrêt Pelletier du Tribunal des conflits du 30 juillet 1875 pose le principe selon lequel le fonctionnaire ne peut voir sa responsabilité personnelle mise en cause devant le juge civil qu'autant qu'il aurait commis une faute se détachant du service, c'est-à-dire une faute personnelle.

b) Procédure

Les tribunaux d'instance ou de grande instance de l'ordre judiciaire sont dans ce cas appelés à juger de la mise en œuvre de la responsabilité civile des fonctionnaires. Le délai de prescription est de trente ans.

2.2.3 La mise en œuvre de la responsabilité punitive

A) La mise en œuvre de la responsabilité pénale

a) La mise en œuvre de la responsabilité pénale de l'établissement

Depuis le 1er mars 1994, les personnes morales de droit public, à l'exception de l'Etat, peuvent faire l'objet d'une condamnation pénale. Deux conditions cumulatives doivent être réunies pour que la responsabilité d'un établissement de santé soit mise en jeu :

- l'infraction doit être commise pour le compte de l'établissement, ce qui signifie que l'infraction ne peut être imputable à l'établissement que s'il en résulte pour lui un certain avantage, matériel ou moral. Les actes accomplis dans l'intérêt personnel d'un agent ou dans celui d'autrui n'engagent pas la responsabilité de l'établissement.

- l'infraction doit être commise par les représentants ou les organes de l'établissement.

La responsabilité pénale de la personne morale ne peut être engagée qu'à l'occasion d'une décision ou d'un acte effectués par ses représentants ou ses organes, ce qui concerne le Conseil d'administration, son Président ou le Directeur. La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques, auteurs ou complices des mêmes faits.

b) La mise en œuvre de la responsabilité pénale personnelle

La responsabilité pénale des fonctionnaires a été reconnue par le Tribunal des conflits en 1935[29]. Ainsi, une faute constitutive d'une infraction pénale autorise la mise en jeu de la responsabilité pénale de l'agent et non celle de l'administration, qu'elle revête ou non le caractère d'une faute personnelle. La notion de faute détachable ou non détachable de la fonction est étrangère au domaine de la responsabilité pénale. La mise en cause pénale du directeur d'hôpital suppose l'existence d'une infraction, d'un comportement fautif dont la preuve doit être rapportée devant les juges répressifs. La faute peut résulter d'un acte délibéré ou d'un acte involontaire aux conséquences dommageables. Dans le domaine hospitalier, la notion de faute involontaire peut être assimilée au manquement à une obligation de sécurité. Pendant longtemps, ce manquement a été associé aux délits d'homicide involontaire[30] ainsi qu'aux coups et blessures involontaires[31]. Plusieurs directeurs d'hôpital ont été condamnés sur le fondement de l'homicide involontaire :

- Le tribunal de grande instance de la Seine a condamné le directeur d'un établissement à un mois de prison avec sursis et 3000 F d'amende à la suite du décès d'un patient dû à l'interversion des canalisations d'oxygène et de protoxyde d'azote. Le juge pénal a considéré que le directeur avait commis une faute en ne respectant pas un arrêté ministériel qui oblige la réception des installations d'oxygène par une commission de sécurité[32].
- La cour d'appel de Bordeaux a condamné un directeur à 2000 F d'amende pour n'avoir pas respecté l'obligation de contrôle et de sécurité qui s'impose à lui. Dans cette affaire où une patiente était décédée par électrocution, le directeur, informé de la défectuosité d'un bistouri électrique n'avait pas transmis au chirurgien le rapport de l'organisme de contrôle et n'en avait pas l'utilisation de ce matériel[33].

---

[29] TC 14 janvier 1935, *Thépaz*

[30] article 221-6 du code pénal

[31] articles 222-19 et 222-20 du code pénal

[32] TGI La Seine, 6 décembre 1966

[33] CA Bordeaux, 25 janvier 1984

Le nouveau code pénal entré en vigueur le 1er mars 1994 a proposé de nouvelles incriminations qui étendent le champ d'intervention du juge pénal dans le domaine de l'administration. L'agent public présumé coupable d'un manquement à une obligation de sécurité ou de prudence ne s'expose plus seulement à des poursuites en cas d'atteinte à la vie ou à l'intégrité physique des personnes. Certains dommages aux biens peuvent désormais fonder la sanction. Le code pénal prévoit même la possibilité de sanctionner des manquements à une telle obligation de sécurité ou de prudence en l'absence de toute conséquence dommageable.

- L'article 223-1 institue l'infraction de mise en danger d'autrui. L'objet de cette infraction est de sanctionner un comportement susceptible d'entraîner un dommage, une catastrophe.
- L'article 223-7 sanctionne l'abstention de combattre un sinistre ou de supprimer un danger pour la sécurité des personnes.
- L'article 322-5 punit la dégradation ou destruction volontaire par l'effet d'une explosion ou d'un incendie.

Cette extension de l'obligation de sécurité étant susceptible d'entraîner de nombreuses mises en cause d'agents publics, la loi du 13 mai 1996 inscrit dans le code pénal le principe général de l'appréciation in concreto de la faute par imprudence.

B) Les conditions de la mise en œuvre de la responsabilité pénale

a) Les conditions restrictives de l'acceptation de l'« excuse budgétaire »

Seul peut être considéré comme fautif le comportement qui n'est pas celui d'une personne « normalement diligente » au regard des circonstances. Ainsi, même en cas de violation d'une réglementation préexistante, il est possible de débattre de l'existence de la faute au regard des circonstances de l'espèce. Ces dispositions s'appliquent particulièrement à la situation du directeur d'hôpital qui ne maîtrise que très imparfaitement les moyens dont il dispose et qui assume des responsabilités extrêmement diversifiées, ce qui le contraint compte tenu de ses moyens à établir des priorités tout en devant assurer le principe de continuité du service public. Il est donc normal que ces éléments soient pris en compte par le juge pour apprécier si le fonctionnaire a effectivement commis une faute pénale. Pour autant, le directeur d'hôpital confronté à une telle situation ne doit pas se limiter à argumenter l'absence de moyens. Il doit pour exonérer sa responsabilité démontrer qu'il a tout fait pour obtenir des moyens supplémentaires, qu'il a informé son autorité de tutelle et l'administration des risques que créait une telle situation et des moyens nécessaires pour y mettre fin. Ce n'est qu'à cette seule condition qu'il pourra plaider l'excuse budgétaire devant le juge.

b) La délégation de signature ne libère le délégant de sa responsabilité que dans certaines situations

La délégation de signature est consentie à une personne nominativement désignée. Elle prend fin lorsque le délégant ou le délégataire change. Sauf texte contraire, le titulaire d'une délégation peut à son tout procéder à une délégation des compétences qui lui ont été confiées. La délégation de signature ne modifie pas le titulaire de la compétence. Le délégant peut à tout moment décider aux lieu et place du délégataire. Les décisions prises par le délégataire sont réputées prises par le délégant. Au regard du droit pénal cependant, le principe est que nul n'est responsable que de son propre fait. Par suite, la responsabilité du délégataire qui commet directement l'infraction sera nécessairement engagée. La responsabilité du délégant n'est donc pas automatique. Toutefois, la délégation peut être la source de l'engagement de la responsabilité du délégant. En matière de sécurité, l'existence d'une intention n'est pas une condition de la constitution de l'infraction. Chaque responsable doit apporter l'attention, la rigueur, la vigilance exigées par les textes pour l'accomplissement de sa mission. Si le délégant néglige de surveiller les conditions dans lesquelles la délégation est exercée, sa responsabilité pourra être mise en cause sur le fondement de la négligence fautive, pénalement sanctionnée. Le délégant ne pourra prétendre s'abriter par principe derrière la délégation s'il peut être démontré qu'il avait eu connaissance des imprudences de son délégataire. La responsabilité du délégant sera fonction de la nature et du contexte de sa négligence.

c) Protection du fonctionnaire

La loi du 16 décembre 1996 relative à l'emploi dans la fonction publique et à diverses mesures d'ordre statutaire décide que « la collectivité est tenue d'accorder sa protection au fonctionnaire ou à l'ancien fonctionnaire dans le cas où il fait l'objet de poursuites pénales à l'occasion de faits qui n'ont pas le caractère d'une faute personnelle ».

2.3 La gestion du risque informatique contribue à l'accomplissement des missions du service public hospitalier dans des conditions de qualité et d'économie optimisées

2.3.1 L'amélioration des performances du SIH ne peut s'envisager sans sécurité

A) La sécurité du SIH bénéficie au patient

Le développement du système d'information est un facteur d'amélioration de la qualité des soins mais n'est acceptable sans que des mesures de sécurité adaptées soient prises.

a) L'ouverture du système d'information et ses perspectives d'évolution rendent nécessaire la prise en compte des risques

Le besoin de partager l'information augmente et s'impose. Il en va ainsi des protocoles communs, des réseaux de prise en charge, des guides de bonne pratique. La solution pour améliorer significativement la qualité des soins semble de plus en plus passer par des échanges d'informations médicales entre les professionnels de santé. Le travail coopératif est devenu un outil stratégique car il répond également à des raisons d'amélioration de la productivité et de réduction des coûts en limitant par exemple les hospitalisations inutiles ou les examens redondants.

L'évolution des pratiques conduit à une mutation des systèmes d'information hospitaliers pour une intégration dans des systèmes d'information de santé. « Le modèle de prise en charge et de décision devient un modèle de partage de compétences après une information sur les choix envisageables, une discussion sur les options possibles avec le patient et/ou les collègues soignants, une délibération pré-décisionnelle basée sur les référentiels de guides de bonne pratique avant une prise de décision partagée avec le patient. »[34]. Ce modèle nécessite la construction de systèmes d'information puissants faisant appel à la normalisation et à l'application de standards qui demandent la structuration des données, la définition des messages, des protocoles d'échange. L'interopérabilité des systèmes d'information demande également un codage des données suivant des normes et standards. Ainsi la norme DICOM pour l'échange d'images numérisées. La mise en œuvre de ces standards est un objectif majeur même si

[34] FIESCHI M., *Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins*, 2003. Rapport au ministre de la santé, de la famille et des personnes handicapées

des échanges sont déjà possibles dans des conditions de sécurité relativement satisfaisantes. Ce n'est que dans ces conditions que le dossier commun du patient informatisé pourra se mettre en place.

b) La sécurité de l'information profite à la sécurité des soins

La nécessité de disposer d'outils d'assurance qualité conçus pour améliorer les processus de soin et leurs résultats s'impose. Ces outils exigent la mise en œuvre de systèmes d'information adaptés. La fréquence croissante des mises en cause des médecins dans leurs pratiques augmente. Les praticiens doivent donc justifier et expliquer leurs choix. L'identification des erreurs humaines et de leurs conséquences dans le domaine médical demande un effort de saisie des informations pertinentes en temps réel sur le lieu où elles sont produites pour les transmettre dans le cadre des systèmes de vigilance et de traçabilité. Cela induit une approche dans laquelle les technologies de l'information deviennent une composante déterminante du management de la sécurité des patients.

La sécurisation du SIH permet aussi de mettre en œuvre des outils contribuant à la performance des soins. Deux exemples peuvent permettre d'illustrer cette affirmation.

Le développement de la télémédecine pour élargir l'offre de soins et le développement des soins à domicile est très souhaitable. Il est un facteur d'amélioration de la qualité de la prise en charge des patients. Les outils de la télémédecine sont majoritairement des outils de communication, comme la vidéoconférence et la téléexpertise. Le CH de Dreux transmet par exemple des images numérisées vers le CHU de Rouen pour interprétation. La qualité de l'image transmise joue dans ce cas un rôle important. La perte de qualité lors de la transmission peut en effet fausser un diagnostic.

L'utilisation des bases de connaissances informatisées permet une aide à la décision. Des organismes multiples, qu'ils soient nationaux, comme l'ANAES, ou internationaux, élaborent des guides de bonnes pratiques dont la mise en œuvre et l'accès rapide peuvent être facilités par les systèmes d'information.

Cependant, ces outils créent une dépendance vis-à-vis du système d'information qui augmente l'impact des risques.

c) Anticiper le partage des données de santé

La loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé a rappelé la place du patient et son rôle dans le système de soins. Elle autorise l'hébergement de «données de santé à caractère personnel recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins ». Cet ensemble inclut les données du dossier médical hospitalier, mais aussi les informations médicales

détenues par les professionnels de santé en dehors de l'hôpital. Certains projets proposent une vision encore plus large, qui intégrerait dans ce dossier dématérialisé des données mises à jour par le patient lui-même ou des données inscrites par un professionnel pour son propre usage.

Depuis la loi du 4 mars 2002, une personne ou une entreprise ne peut commencer une activité d'hébergement qu'après avoir obtenu l'agrément de l'administration. Les conditions de cet agrément doivent être définies par un décret en Conseil d'Etat pris après avis de la CNIL et des conseils de l'ordre des professions de santé et paramédicales. A l'heure actuelle, ce décret n'est toujours pas paru et la date de sa parution semble assez lointaine. La loi prévoit néanmoins un régime transitoire qui permet aux personnes ou aux sociétés qui l'exerçaient déjà avant la parution de la loi de continuer à l'exercer. Des sociétés commerciales spécialisées dans la gestion des données médicales sur Internet se sont en effet déjà positionnées sur ce marché, ce qui a obligé la CNIL, qui reçoit obligatoirement le formulaire de déclaration préalable, à intervenir pour imposer des critères de qualité en matière de chiffrement des données, de définition claire d'une politique d'accès aux données et de conditions de sécurité mises en place par la société.

Dans ce nouveau contexte, le patient devient un acteur essentiel dans le monde médical. Il a non seulement un véritable droit d'accès à l'information médicale personnelle, mais en outre la loi du 4 mars 2002 le place au centre du contrat d'hébergement. Il a la possibilité de prendre l'initiative de faire héberger son dossier médical chez l'hébergeur de son choix. Dans cette hypothèse, qui devrait être dans un premier temps la moins courante, il est évidemment au centre du contrat. Dans le cas où l'initiative est prise par un professionnel de santé, il doit donner son accord après avoir été averti des risques liés à la dématérialisation et à la confidentialité des informations.

Les Centres hospitaliers seront pour la plupart amenés petit à petit à mettre en place ce dossier du patient informatisé. Le CH de Dreux commence à s'en donner les moyens. Cependant, pour exercer cette fonction d'hébergeur de données de santé, la soumission à l'agrément est nécessaire. Le décret n'étant pas encore paru, les conditions qu'il pose ne sont pas connues précisément mais il est déjà acquis que des contrats types d'hébergement seront mis en place et que des modalités techniques de la protection des informations seront exigées. Les hébergeurs seront soumis au contrôle de l'IGAS et des agents du ministère de la Santé. Des sanctions sont même déjà prévues, parmi lesquelles figurent le retrait de l'agrément administratif et des sanctions pénales.

La mise en place d'une politique de sécurité informatique participe déjà à la préparation de cette nouvelle activité.

B) Un juste compromis doit être trouvé entre les performances du système d'information et sa sécurité

a) L'ergonomie et l'accessibilité ne doivent pas être négligées

Le facteur humain est central dans la mise en place de systèmes sécurisés, dans leur cycle de vie et dans leur utilisation. Alma Whitten a ainsi publié en 1998 un article intitulé « why Johnny can't encrypt »[35] qui montre bien la difficulté de concilier sécurité des systèmes d'information et facilité d'utilisation. Cette chercheuse américaine a demandé à une série d'étudiants habitués à manipuler un ordinateur d'utiliser un logiciel de cryptographie pour envoyer un courrier électronique sécurisé à un correspondant. Bien qu'ayant à leur disposition un ordinateur où tous les logiciels étaient parfaitement installés, ainsi que les manuels du logiciel de cryptographie, aucun parmi la vingtaine d'étudiants n'a réussi à envoyer le message crypté au bout d'une heure et demie d'essais. Plus de la moitié avaient même envoyé le message en clair sans s'en rendre compte. Ainsi, il semble qu'il existe une limite au-delà de laquelle on ne peut augmenter la sécurité d'un système sans diminuer sa facilité d'utilisation. Un système facile à utiliser ne peut pas être sûr et un système sûr est difficile à utiliser. Une analyse des risques minutieuse est donc nécessaire pour déterminer le juste dimensionnement de la politique de sécurité.

b) Une politique de sécurité trop contraignante risque de créer un écart entre la théorie et les pratiques des professionnels

Il semble en effet acquis qu'une politique de sécurité trop stricte sera contournée par les utilisateurs, ce qui est contre-productif à un double titre. D'une part, l'accroissement du niveau de sécurité se traduit par des coûts supplémentaires plus que proportionnels. Et d'autre part, c'est l'ensemble de la sécurité d'un système installé qui peut être anéanti par une seule décision des acteurs de ce système.

c) La mise en place du dossier patient informatisé doit concilier rentabilité économique et déontologie médicale

Il est désormais admis qu'il y ait une justification macro-économique, voire micro-économique pour certains économistes de la santé, à l'utilisation des technologies de l'information et de la communication dans le domaine de la santé. La modification des pratiques, les exigences de la sécurité, la maturité des technologies et la baisse de leurs coûts sont autant d'arguments qui plaident en la faveur de la rentabilité de ces nouvelles

[35] WHITTEN A., TYGAR J.D. *Why Johnny can't encrypt*. http://www.cs.cmu.edu/~alma/johnny.pdf

technologies à l'hôpital. Des études américaines montrent en effet que les hôpitaux qui ont choisi de mettre en œuvre des solutions utilisant intensivement les technologies de l'information et de la communication contrôlent mieux leurs dépenses et ont une meilleure productivité que les hôpitaux qui n'ont pas eu cette stratégie[36]. Il semble que la mise en œuvre des dossiers informatisés pour des malades traités en ambulatoire entraîne un retour sur investissement positif. La mise en place du partage des données de santé devrait amener des économies que certains experts fixent entre 20 et 30% des coûts totaux. Cependant, compte tenu du nécessaire respect de la législation relative aux droits des patients, ces technologies ne peuvent être déployées sans une politique de sécurité adaptée et sans garantie du respect des règles déontologiques.

Les professionnels de santé vivent avec le développement des technologies de l'information et de la communication un bouleversement de leurs pratiques. Le partage de l'information qui est désormais facilité, au-delà des problèmes techniques ou méthodologiques, pose des questions psychologiques et culturelles. Les professionnels de santé, très attachés au secret médical et à l'exercice individuel de la médecine, ne peuvent adhérer au partage des données des patients qu'à la condition que des garanties de sécurité sont apportées et si l'organisation mise en place est transparente et garante du respect de leurs pratiques.

2.3.2 La démarche qualité doit prendre en compte la sécurité du système d'information dans l'ensemble de ses aspects

A) Gestion des risques et qualité : des démarches proches

a) Les liens entre les notions de qualité et de sécurité sont étroits

Démarche qualité et gestion des risques sont intimement liées. « La mise en place dans un établissement d'une politique de gestion des risques procède justement de ce que plus le niveau de risque baisse, plus celui de la qualité augmente »[37]. Inversement, l'amélioration continue de la qualité est une stratégie efficace d'amélioration de la sécurité. La réunion dans le manuel d'accréditation des deux démarches dans un référentiel unique intitulé « Qualité et Prévention des Risques » prouve leur interdépendance. La démarche qualité est par excellence transversale et ne peut se

[36] SOLOVY A. *The big payback : survey shows a healthy return on investment for the info tech.* Hospitals & Health Networks, juillet 2001, pp 40-50

[37] ROUAULT B., Sûreté de fonctionnement et patrimoine hospitalier : une méthode de gestion des risques au service du décideur. ENSP, mémoire, 1997

concevoir sans une réflexion globale sur les processus. Pendant longtemps cependant, les efforts sont restés cloisonnés et axés sur des domaines particuliers. La gestion des risques a jusqu'à une date récente été cantonnée dans la mise en œuvre des vigilances obligatoires, ce qui n'a pu conduire à une véritable intégration dans une stratégie globale. Les experts visiteurs de l'ANAES sont particulièrement attentifs à la mise en place de cette politique de gestion des risques qui aide au développement d'une culture qualité dans les établissements de santé.

b) Les méthodes utilisées sont proches

La démarche qualité s'appuie sur un noyau de méthodes proches ou similaires à la gestion des risques. Toutes deux se basent sur l'analyse des processus et sur des méthodes de résolution de problèmes. Dans les deux cas, l'analyse des incidents n'est plus centrée uniquement sur l'erreur, sur la faute, mais elle l'est aussi sur la recherche d'insuffisances dans le système qui ont permis à l'erreur humaine, à la panne de dégénérer en accident. Les facteurs de réussite des deux démarches sont donc voisins et reposent sur la détermination d'une politique claire et engagée par la direction générale, sur la définition des responsabilités des acteurs de cette politique et sur l'implication de chacun.

B) La gestion du risque informatique dans la procédure d'accréditation

L'ordonnance du 24 avril 1996 a fait de la qualité et de la sécurité un objectif stratégique des hôpitaux. L'engagement dans une procédure d'accréditation est une obligation pour l'ensemble des établissements. L'article L.6113-7 du CSP dispose ainsi qu' « afin d'assurer l'amélioration continue de la qualité et la sécurité des soins, tous les établissements de santé publics et privés doivent faire l'objet d'une procédure externe d'évaluation appelée accréditation ». L'article L. 6114-3 modifié par l'ordonnance n°2003-850 du 4 septembre 2003 précise que les contrats d'objectifs et de moyens conclus avec l'ARH « définissent les objectifs en matière de qualité et de sécurité des soins ».

a) Le manuel d'accréditation de l'ANAES

Le manuel d'accréditation des établissements de santé impose la prise en compte de la sécurité des systèmes d'information et de la confidentialité des données. De manière large, on peut considérer que le référentiel gestion des fonctions logistiques dans ses références 5 (relative au nettoyage des locaux et des équipements) et 9 (relative à l'organisation de la sécurité incendie) contribue, par son action sur l'environnement du système informatique, à sa sécurité. Plus précisément, le référentiel gestion du système d'information traite de la politique de sécurité informatique, de manière indirecte dans les

références 1 et 4 et de façon directe dans la référence 2 intitulée « les mesures nécessaires à la protection de la confidentialité, à la sécurité des informations concernant les patients et au respect de leurs droits dans la gestion de l'information sont prises ». Quant à la politique de gestion du risque informatique, elle peut trouver des bases dans le référentiel Gestion de la qualité et des risques, en particulier dans le référentiel 4 concernant le programme de prévention des risques.

GESTION DES FONCTIONS LOGISTIQUES	
GFL – référence 2	**L'établissement est organisé pour assurer la sécurité et la maintenance des bâtiments, des équipements et des installations**
GFL 2.a.	L'établissement met en œuvre les recommandations issues des contrôles externes des bâtiments, et équipements
GFL 2.b.	Une politique de maintenance est définie
GFL 2.c.	Une maintenance préventive est assurée
GFL 2.d.	Une maintenance curative est assurée
GFL 2.e.	Des protocoles d'alerte et d'intervention sont écrits et connus des personnels concernés
GFL – référence 8	**L'établissement dispose d'une organisation et de personnels chargés d'assurer la sécurité des biens et des personnes**
GFL 8.b.	L'établissement met en œuvre des mesures préventives pour assurer la sécurité des personnes
GFL 8.c.	Des protocoles d'alerte sont rédigés et connus de tous
GFL – référence 9	**L'établissement est organisé pour assurer la sécurité des personnes contre l'incendie**
GFL 9.a.	L'établissement s'assure du passage à la commission de sécurité et en suit les recommandations
GFL 9.b.	L'établissement a mis en place une organisation pour prévenir le risque incendie
GFL 9.c.	Les professionnels bénéficient d'une formation incendie actualisée
GFL 9.d.	Les protocoles d'alerte et les mesures à prendre en cas d'incendie sont écrits et connus de tous les professionnels
GESTION DU SYSTEME D'INFORMATION	
GSI - référence 1	**Une politique des systèmes d'information est définie et mise en œuvre**
GSI 1.a.	Le système d'information et l'informatisation de l'établissement sont fondés sur un schéma directeur, cohérent avec le projet d'établissement et élaboré de manière participative
GSI 1.b.	Le système d'information couvre l'ensemble des activités de l'établissement et favorise une approche et une utilisation coordonnées et efficaces de l'information, notamment pour la politique d'évaluation
GSI 1.c.	Les instances concernées sont impliquées dans le suivi du schéma directeur de l'information
GSI – référence 2	**Les mesures nécessaires à la protection de la confidentialité, à la sécurité des informations concernant les patients et au respect de leurs droits dans la gestion de l'information sont prises**
GSI 2.a.	Une politique est définie, conduite et connue des professionnels en ce qui concerne la protection de la confidentialité des informations concernant les patients
GSI 2.b.	La sécurité des données et de leur accès est organisée
GSI 2.c.	Tous les traitements informatisés nominatifs sont déclarés à la CNIL
GSI – référence 4	**Le système d'information répond aux besoins des professionnels utilisateurs et fait l'objet d'une politique d'amélioration de la qualité**
GSI 4.a.	Une procédure régulière visant à recueillir des informations sur les besoins, l'avis et la satisfaction des professionnels utilisateurs est en place

GSI 4.b.	Les dysfonctionnements du système d'information sont recensés, analysés et traités
GSI 4.c.	Un plan d'amélioration de la qualité du système d'information, aux priorités hiérarchisées et auquel participent les professionnels utilisateurs, est en place
GESTION DE LA QUALITE ET PREVENTION DES RISQUES	
QPR – référence 1	**L'établissement initie, pilote et soutient une politique qualité s'appuyant sur la gestion de la qualité et la prévention des risques**
QPR 1.b.	La politique qualité comporte des objectifs précis, mesurables dans le temps, traduits dans le programme de gestion de la qualité et prévention des risques
QPR 1.e.	Les responsabilités concernant la gestion de la qualité et la prévention des risques sont identifiés
QPR – référence 4	**Un programme de prévention des risques est en place**
QPR 4.a.	Les informations disponibles relatives aux risques et aux événements indésirables sont rassemblées
QPR 4.b.	Un système de signalement des événements indésirables est en place
QPR 4.c.	Les événements indésirables sont analysés et les mesures d'amélioration des risques
QPR 4.d.	Les secteurs, pratiques, actes ou processus à risque sont identifiés et font l'objet d'actions prioritaires dans le programme de prévention des risques

b) L'enjeu de la prochaine procédure d'accréditation pour le CH de Dreux

Le CH de Dreux s'est engagé très tôt dans la procédure d'accréditation. La demande auprès de l'ANAES a été faite dès le 23 septembre 1999 et la visite des experts-visiteurs s'est effectuée du 23 au 26 mai 2000. A l'issue, le collège de l'accréditation a relevé certaines insuffisances qui ont donné lieu à une réserve majeure.

- les systèmes informatiques existants n'étaient pas interfacés et certains services n'étaient pas équipés.
- Il n'existait pas de véritable service informatique
- la sécurité des données informatiques et leur confidentialité ne semblaient pas assurées dans la pratique
- les déclarations à la CNIL n'ont pas pu être produites aux experts-visiteurs.

De manière plus générale, le Collège de l'accréditation a relevé l'absence d'une véritable politique globale de gestion des risques.

Une visite ciblée a eu lieu le 18 décembre 2002, portant notamment sur cette réserve majeure. A l'issue de cette visite, le Collège de l'accréditation a décidé de lever la réserve majeure.

La prochaine visite des experts-visiteurs aura lieu en 2005. Les référentiels Gestion des systèmes d'information et gestion de la qualité et des risques n'ont pas évolué dans la dernière version du manuel datant de juin 2003. En revanche, l'esprit de l'accréditation qui se révèle à travers les introductions de ces deux chapitres est bien d'une part d'ouvrir le système d'information en interne comme en externe, et d'autre part de mettre en œuvre

une véritable politique de gestion des risques centralisée pour contrebalancer l'exposition plus grande aux risques.

C) La qualité du système d'information et la prévention des risques peut passer par l'engagement de l'établissement de respecter des normes reconnues

a) Les normes existantes

Si la réglementation relative à la sécurisation des systèmes d'information hospitaliers s'imposant aux établissements de santé est inexistante, en revanche il existe plusieurs normes établies par divers organismes nationaux ou internationaux. L'abondance de ces normes est d'ailleurs souvent source de confusion et d'embarras. Pourtant le choix d'une ou plusieurs normes et méthodes d'organisation ou d'évaluation de la sécurité s'avère indispensable pour mettre en place une politique de sécurité cohérente, homogène et efficace. Un certain nombre d'avantages peuvent en être attendus, dont une liste est proposée ci-dessous.

- obtenir une vision globale et cohérente de la sécurité
- fournir un référentiel et des concepts communs à tous les acteurs, permettant les audits de ce référentiel
- fournir un cadre commun pour gérer les risques
- proposer des parades adaptées aux risques
- améliorer la sensibilisation des utilisateurs
- prendre en compte la sécurité dans la gestion des projets
- favoriser la démarche qualité
- éventuellement faire baisser le coût des assurances.

De manière générale, les normes ISO 9001 comprennent des volets s'appliquant à la sécurité du système d'information. Il existe cependant des normes plus spécifiques qui peuvent être adaptées sans trop de difficultés aux hôpitaux.

La plus connue est sans doute la norme ISO 17799, Code of practice for information security management, publiée en décembre 2000. Cette norme d'origine britannique (BS7799) a bénéficié d'une forte médiatisation et est souvent citée en référence. Il s'agit d'une norme générale s'appliquant à l'ensemble des structures disposant d'un système d'information. Cependant, son adaptation aux établissements de santé ne pose pas de difficultés particulières. La preuve en est que les principes et règles de mise en œuvre d'une politique de sécurité cadre des systèmes d'information des établissements de santé édités par le GMSIH en sont directement issus.

Le CEN a élaboré sous la référence ENV12924 une classification des systèmes d'information de santé en fonction du niveau de risque auxquels ils sont exposés. A cette classification correspondent des mesures de protection, parmi lesquelles il conviendra de choisir selon les recommandations des instances de normalisation. La méthodologie suivie pour l'élaboration de la classification des systèmes d'information repose sur les résultats d'audits de plusieurs systèmes d'informations européens. Les résultats de cette enquête ont été compilés et ont permis d'élaborer une classification en six catégories selon leur sensibilité au regard des propriétés fondamentales de la sécurité (disponibilité, confidentialité, intégrité).

b) Vers une certification des SIH ?

Une certification est délivrée par un organisme indépendant et permet d'attester la conformité d'un produit, d'un système ou d'un service à des exigences bien définies comme, par exemple, celles de l'ISO 9001 (exigences pour les systèmes de management de la qualité) ou de l'ISO 14001 (exigences pour les systèmes de management de l'environnement). Elle s'appuie sur un audit « tierce partie », c'est-à-dire un audit réalisé par un organisme externe indépendant de toute partie ayant un intérêt dans l'entité auditée.

En tant que code de bonnes pratiques pour le management de la sécurité de l'information, l'ISO 17799 ne définit aucune exigence en matière de produit, de système ou de service. Une certification par rapport à cette norme n'est donc pas possible. Toutefois, le British Standard Institute a rédigé une seconde partie à la norme BS7799 qui est à l'origine de l'ISO 17799 qui peut être utilisée pour auditer et certifier un système de management de la sécurité de l'information. Ainsi, les établissements de santé qui le désirent vont pouvoir bientôt s'engager dans des démarches de certification de leurs systèmes d'information. L'intérêt de le faire ne repose pas sur la preuve de l'invulnérabilité du système d'information, ce qui n'est pas l'objet de la certification, mais permet de motiver le personnel, de l'inciter à formaliser des procédures et à les respecter, ce qui au final contribue à la sécurité. De plus, la certification est le moyen de faire connaître au personnel, au public, aux tutelles et aux assureurs que l'établissement s'impose des règles de bonnes pratiques et va au-delà du strict respect de la réglementation. Cette démarche contribue à améliorer l'image de l'établissement et comporte un intérêt économique à ne pas négliger.

2.3.3 Les enjeux économiques d'une politique de sécurité informatique

A) Préserver le patrimoine de l'établissement

a) Les ressources informatiques représentent une valeur financière

Alors qu'ils constituaient il y a quelques années une partie peu importante du patrimoine de l'établissement, les équipements et logiciels informatiques en représentent aujourd'hui une part non négligeable qu'il convient de protéger. Pour preuve, l'achat cette année de deux serveurs équipés et d'un logiciel de gestion de base de données a représenté un coût de près de 250 000 €, tandis que le coût du progiciel de gestion administrative et médicale additionné à celui de gestion des urgences a constitué un investissement d'environ 1050 000 €. Ces ressources, de même que le parc de près de 600 micro-ordinateurs, sont à maintenir et à protéger car elles ont une valeur importante, même si les biens informatiques connaissent une obsolescence rapide.

b) La qualité des informations médico-administratives a déjà un impact sur le budget de l'établissement

La législation hospitalière oblige les établissements de santé, publics et privés, à procéder à l'analyse de leur activité. Ils doivent notamment mettre en œuvre des systèmes d'information tenant compte des pathologies et des modes de prise en charge des malades[38]. Ces systèmes d'information doivent permettre aux établissements de santé de procéder à la synthèse et au traitement informatique des données médicales. A cet effet, les praticiens de tous les établissements de santé sont tenus de transmettre à un médecin de l'établissement responsable de l'information médicale, les données de nature médicale nécessaires au suivi et à l'analyse de l'activité[39]. Outil de gestion, l'information médicale doit permettre par une connaissance fine de l'activité hospitalière, une meilleure gestion interne des établissements et surtout l'exercice « médicalisé » par les autorités de tutelle du contrôle sur les établissements de santé et sur les moyens qui leur sont alloués.

Le PMSI organise la production, pour chaque séjour d'un malade dans un établissement hospitalier, d'un résumé de sortie standardisé (RSS) comprenant un résumé administratif et, selon que le patient a été hospitalisé dans une ou plusieurs unités médicales, un ou plusieurs résumés d'unités médicales cliniques (RUM). Les médecins chargés des unités médicales concernées établissent les RSS sous leur responsabilité, en codant les informations médicales relatives à chaque malade. Chaque malade hospitalisé se trouve

[38] article L. 6113-7 du CSP

ainsi classé à l'issue de chacun de ses séjours, à partir de son diagnostic principal, des diagnostics associés et de certains actes médicaux significatifs, dans un groupe homogène de malades (GHM). L'activité des établissements peut dès lors être décrite en dénombrant le nombre de séjours par GHM. Les données ainsi recueillies permettent de calculer pour chaque GHM des coûts de référence nationaux établis à partir des données fournies par un échantillon d'hôpitaux. Chaque GHM se voit attribuer un certain nombre de points ISA (indicateur synthétique d'activité). Il est ensuite possible, connaissant le nombre de patients traités dans chaque GHM au sein de l'hôpital, le nombre de points ISA correspondant à ce GHM, ainsi que le budget de l'établissement, de calculer la valeur en euros du point ISA de l'hôpital et, par conséquent, d'établir des comparaisons entre les différents établissements.

L'ordonnance hospitalière du 24 avril 1996 prévoit que parmi les critères d'allocation des ressources aux établissements publics de santé par le directeur de l'ARH figurent les données de l'activité médicale. La qualité des informations codées revêt donc une importance budgétaire et stratégique considérable que la mise en œuvre de la tarification à l'activité va encore renforcer.

c) La tarification à l'activité va renforcer la valeur financière des informations produites par le système de santé

L'un des volets du plan Hôpital 2007 vise en effet à rapprocher les modes de financement des établissements publics et privés en s'appuyant sur le recueil des de l'information du PMSI. L'allocation des ressources s'orientera dès janvier 2004 vers une tarification à l'activité pour les activités de médecine, de chirurgie et d'obstétrique. Ce financement distinguera les missions de soins qui ont vocation à être financées directement à l'activité sur la base du PMSI par groupe homogène de séjour, et les missions d'intérêt général et d'aide à la contractualisation (MIGAC), qui seront financées par une dotation. Le changement des règles de financement se fera par étapes, la part de financement garantie diminuant progressivement par rapport à la part facturée aux séjours ou aux actes. Cette répartition des deux modes de financement sera fixée chaque année par le Ministre chargé de la santé. En 2004, à partir du second semestre, le versement des recettes sera encore globalisé sous forme de dotation globale et il ne sera tenu compte de l'activité que pour 5 à 10% de l'enveloppe MCO. A compter de 2006, la part de l'activité MCO soumise à la tarification à l'activité atteindra 20 à 30%, ce qui représentera une masse budgétaire non garantie d'environ 20 millions d'euros pour le CH de Dreux.

---

[39] Loi n°93-121 du 27 janvier 1993

Dans ce nouveau contexte budgétaire, l'information prend une valeur financière déterminante. Les erreurs de codage peuvent avoir des implications non négligeables et il est nécessaire que le recueil des RSS gagne en exhaustivité et en qualité. De plus, le financement de l'activité étant lié aux données d'activité fournies par les établissements, il devient nécessaire afin d'optimiser la trésorerie de l'établissement de raccourcir le délai de production des RSS. Or, plus de la moitié des établissements considèrent qu'il n'est pas possible dans la situation actuelle de raccourcir à un mois après la sortie du patient la production des RSS, notamment en raison du délai incompressible des contrôles et des services retardataires. Une vigilance particulière sera nécessaire en 2004 du fait de la concomitance d'une autre réforme d'importance. Le passage au codage des actes selon une nouvelle nomenclature, la CCAM, constitue un bouleversement important du système d'information des établissements et des pratiques professionnelles. Le CH de Dreux disposera pour juillet 2004 des outils informatiques nécessaires à la mise en place de la CCAM et a commencé à former ses médecins à cette nouvelle pratique de codage. Néanmoins, ce changement nécessite une phase d'adaptation propice aux erreurs.

B) Favoriser l'assurabilité de l'établissement

a) Contexte du marché de l'assurance des hôpitaux en matière de responsabilité civile

La loi du 4 mars 2002 relative aux droits des malades a créé une obligation d'assurance des établissements de santé. Cependant, face à l'augmentation significative du contentieux liée à l'activité médicale, un certain nombre d'assureurs ont préféré arrêter leur activité de responsabilité civile. Ainsi, en juillet 2002, l'assureur américain ACE s'est retiré du marché, à la suite de Saint Paul. Le marché de l'assurance est donc devenu un marché quasi-monopolistique dominé par la Société hospitalière d'assurances mutuelles (SHAM), dans lequel les hôpitaux subissent des primes élevées. Le CH de Dreux a ainsi connu une augmentation de sa prime de près de 40% en 2003, ce qui est encore « raisonnable » par rapport à la moyenne des établissements de santé. Les assurances de dommage aux biens connaissent elles aussi une tendance à la concentration des offres et donc au renchérissement. Les préjudices causés aux patients du fait de la survenue d'un risque lié au système d'information sont encore très rares et souvent liés à d'autres causes. La prévention de ces risques complète néanmoins une politique globale de gestion du risque et à ce titre peut contribuer à faire diminuer la prime d'assurance.

b) Les contrats actuels en matière informatique

Le besoin de protection s'exprime aussi à travers la recherche d'une assurance du risque informatique, complétant la sécurité qu'apporte la maintenance. L'assurance complète la maintenance, qui elle-même influence le risque assuré. Le risque informatique n'est pas facile à cerner. L'intrusion de l'immatériel complique les choses. L'assurance des machines ne compte en effet plus guère. L'important est désormais de prendre en compte les richesses immatérielles, c'est-à-dire les données, ainsi que les dommages qu'elles peuvent causer. Or, les contrats actuels en matière informatique ne prennent généralement en compte les dommages immatériels que s'ils sont consécutifs à des dommages matériels, ce qui est loin d'englober tous les risques. En principe, tout est assurable à partir du moment où il existe un aléa. Les actes de malveillance peuvent donner lieu à la souscription d'une police spéciale « extension aux risques informatiques », qui malgré son nom ne traite que des actes de malveillance. Les contrats couvrent les pertes directes et indirectes. Les pertes directes consistent d'abord dans les dommages causés au matériel, mais concernent aussi les atteintes aux logiciels et aux données. Cependant, dans ce cas l'indemnité d'assurance compense les « frais de reconstitution d'informations » si les informations n'ont pas été effacées de façon définitive. Mais le contrat peut subordonner la prise en charge de ces frais au respect par l'assuré de certaines obligations relatives à la sauvegarde des données. Les pertes indirectes renvoient aux conséquences dommageables résultant pour l'utilisateur des perturbations apportées au fonctionnement du système informatique. Il s'agit par exemple des pertes d'exploitation, ou de l'indemnisation du préjudice lié à la perte de notoriété ou de confidentialité. Pour le moment, les assureurs n'offrent pas de couvrir les risques informatiques immatériels comme le déni de service ou l'indisponibilité prolongée de réseau. Toutefois, une société américaine a mis au point un outil de modélisation de ces risques qui consiste en une série d'audits qui donnent lieu à des rapports de synthèse permettant ensuite d'évaluer le risque au regard des préjudices subis.

Ces types de contrats spécifiques à l'informatique sont avant tout destinés à des entreprises commerciales. Cependant, ils sont significatifs d'une évolution et montrent que les assureurs se préoccupent de cette montée des risques informatiques. Les EPS doivent réfléchir à la place qu'occupe leur SIH au sein de leur patrimoine et à la part de risque qu'ils souhaitent assumer directement, confier à la maintenance ou assurer.

C) Préserver et améliorer l'image de marque de l'établissement

Parler d'image de marque et de parts de marché peut paraître surprenant à propos de l'hôpital. Pourtant, les établissements de santé se situent sur un marché concurrentiel. L'ARH est vigilante quant à la satisfaction des besoins sanitaires de l'hôpital dans son

bassin de vie, tant en quantité qu'en qualité et oriente la planification sanitaire en conséquence. Or, cette clientèle bien informée n'est plus captive.

a) Créer un climat serein propice à l'accomplissement des activités de l'établissement

Une politique de gestion du risque informatique efficace doit prendre en compte les exigences psychiques du personnel. La confiance des utilisateurs dans la fiabilité du système informatique ne doit pas être négligée afin que les actes de soin puissent se dérouler dans des conditions optimales. La mise en place d'une politique de sécurité informatique contribue à créer ce climat de confiance. En outre, la majeure partie des actes malveillants provient de l'intérieur même des établissements. L'affichage de la politique de sécurité et la mise en place de dispositifs techniques permettant d'éviter les risques permettent de dissuader les potentiels auteurs de malveillances.

b) Donner confiance aux partenaires de l'hôpital et avoir confiance en eux

La finalité des systèmes d'information doit être la meilleure prise en charge des patients. Avec l'utilisation des technologies de l'information et de la communication, le but est de favoriser la coordination des professionnels de santé et leur coopération au profit de l'amélioration de l'état de santé des malades. Dans ce cadre, la gestion du risque informatique doit permettre en interne de promouvoir la coopération entre les différents services et acteurs de l'établissement. Vis-à-vis de l'extérieur, la mise en place d'une politique de sécurité et la mise en œuvre de mesures de sécurité doit donner confiance à aux partenaires de l'hôpital qui souhaitent échanger des données. Réciproquement, le CH qui a confiance en ses dispositifs de sécurité ne craindra pas le partage de données avec d'autres établissements ou d'autres professionnels et pourra s'intégrer plus facilement dans un réseau ville-hôpital ou hôpital-hôpital.

c) Eviter les coûts liés à la non-qualité et préserver ses parts de marché

Les entreprises du secteur privé ont compris depuis de nombreuses années que la non qualité avait un coût et donc que la mise en place de dispositif d'amélioration de la qualité et de prévention des risques ne contredisait pas l'efficacité économique.

Un sinistre informatique peut en effet engendrer des coûts imprévus parfois considérables.

- Une panne du système informatique peut diminuer, voire empêcher la réalisation de certains actes médicaux. Cela peut être le cas d'actes médico-techniques d'imagerie médicale ou de laboratoire.

- Une défaillance informatique peut entraîner l'achat de matériel de remplacement, ou des frais de location de matériel de remplacement
- Des frais de maintenance corrective peuvent être engagés
- En cas de dommage aux personnes, des frais de justice, voire le versement de dommages intérêts, peuvent être dus.
- Une augmentation des coûts de personnel due au paiement d'heures supplémentaires peut être engendrée en cas de rappel d'agents non prévus au planning pour faire face au sinistre
- Les primes d'assurance risquent d'être revues à la hausse après un sinistre important.

La sécurité du système d'information n'est pas directement un critère de sélection de l'hôpital par les patients. En revanche, une défaillance grave dans ce domaine serait à n'en pas douter relayée par la presse locale et aurait un impact fort sur le choix des usagers potentiels.

Elément transversal de son organisation, le fonctionnement du SIH impacte celui de l'établissement tout entier. Devenant un outil stratégique, sa sécurité ne peut plus reposer sur un simple empilement de mesures correctives mais doit faire l'objet d'une réflexion d'ensemble formalisée à travers une véritable politique.

3 LE CENTRE HOSPITALIER DE DREUX DOIT REFLECHIR A LA MISE EN PLACE D'UNE POLITIQUE DE SECURITE DE SON SYSTEME D'INFORMATION

L'ampleur de la tâche que constitue le changement du SIH et les contraintes que représentent la maintenance et l'exploitation du système ont laissé peu de place à la réflexion que requiert la rédaction d'une politique de sécurité. Le manque de formalisation des grandes orientations et des procédures qui en découlent constitue la faiblesse essentielle de la gestion du SIH au CH de Dreux. A court terme, les bases d'une telle politique devront être posées et les étapes de sa mise en œuvre programmées.

3.1 La politique de sécurité doit être strictement dimensionnée

3.1.1 Au regard des missions du service public hospitalier, la gestion des risques sanitaires au sens strict est naturellement prioritaire

La politique de sécurité informatique n'entre pas directement dans le champ des missions du service public hospitalier. L'article L.6111-1 du CSP définit le champ d'intervention des établissements de santé. Cet article prévoit que les établissements de santé, publics ou privés, assurent les examens de diagnostic, la surveillance et le traitement des malades, des blessés et des femmes enceintes en tenant compte des aspects psychologiques du patient ». A cette mission traditionnelle, le législateur a ajouté que ces établissements ont vocation à participer « à des actions de santé publique et notamment à toutes actions médico-sociales coordonnées et à des actions d'éducation pour la santé et de prévention ». Enfin, en application de la loi de « sécurité sanitaire » du 1er juillet 1998, tous les établissements de santé sont tenus de participer à la mise en œuvre du dispositif de vigilance destiné à garantir la sécurité sanitaire, d'organiser en leur sein la lutte contre les infections nosocomiales et autre infections iatrogènes, et de mettre en place un système permettant d'assurer la qualité de la stérilisation des dispositifs médicaux.

La prévention du risque informatique ne fait donc pas directement partie des objectifs assignés au Directeur d'hôpital. Néanmoins, en raison du caractère transversal du SIH et des risques que ferait peser sur les patients un dysfonctionnement grave, il paraît justifié de l'insérer dans un ensemble plus large qui est celui de la démarche qualité et de politique de gestion des risques.

3.1.2 Il existe un risque réel de surdimensionnement de la politique de sécurité

A) Le contexte budgétaire dans lequel évoluent les établissements publics de santé, et notamment le CH de Dreux, incite à privilégier les dépenses structurantes consacrées le plus directement possible aux soins du patient.

Si le changement du SIH est par essence une dépense structurante parce qu'elle oblige à repenser le mode de fonction de l'hôpital, à réfléchir sur les pratiques et parce qu'elle vise à améliorer la prise en charge des patients, il n'en va pas de même des dépenses consacrées spécifiquement à la sécurité.

B) L'aspect stratégique du choix de l'ampleur de la politique de gestion du risque informatique

Les hôpitaux n'ont que très peu de recul par rapport à cet aspect de la problématique. L'engagement dans de telles politiques n'est que très récent et rend improbable toute conclusion sur les gains économiques engendrés.

Il est difficile de calculer le coût du risque et le coût de la prévention. De plus, l'adéquation entre ces deux variables a des conséquences éthiques non négligeables. La gestion du risque apparaît comme un savant compromis entre l'art de dépenser pour la prévention afin de réduire les coûts de la non qualité ou de la non sécurité et le risque financier qui serait de produire de la sur-qualité. La démarche de gestion des risques doit donc prendre en compte la dimension économique. L'arbitrage doit se situer au niveau du rapport coût de la prévention/bénéfice escompté en termes de qualité, d'image, d'économie, etc.

Il reste cependant que l'adéquation entre ce qui est mis en place en termes de prévention et ce qui en résulte directement est très délicate à percevoir. La prévention est difficilement mesurable quant à ses effets directs, c'est pourquoi elle est peu privilégiée en France. L'analyse économique du danger peut apparaître comme une aide à la décision et par conséquent à la sélection intelligente des efforts de prévention. Le constat de départ est que le risque zéro est non seulement techniquement impossible à atteindre, mais également trop coûteux. L'enjeu est alors de déterminer la part de risque raisonnable que le décideur hospitalier accepte de prendre et l'effort de prévention optimale. Le danger est aussi de bloquer l'organisation en imposant des barrières systématiques. Ainsi les économistes utilisent l'analyse coût/bénéfice pour évaluer l'efficacité de la prévention. Il s'agit alors de mesurer pour chaque risque identifié le coût de l'effort de prévention envisagé et de le comparer au bénéfice escompté. Il est à noter que pour ce qui concerne l'hôpital, l'analyse du bénéfice attendu ne se limite pas au bénéfice financier mais rend en compte les bénéfices en termes d'amélioration de la satisfaction des patients, de la protection du personnel, de l'image de l'institution, etc…

L'opération intellectuelle semble aisée, mais elle reste très incertaine dans la pratique car l'adéquation entre effort de prévention et bénéfice n'est pas instantanée. Il faut généralement atteindre un certain temps avant de voir si des améliorations sont engendrées. Et souvent ces améliorations ne résultent pas uniquement de cet effort mais elles sont multifactorielles. Ainsi, la stratégie de gestion des risques doit être capable d'aborder cette complexité pour permettre une évaluation de son propre système de prévention.

En tout état de cause, la gestion des risques doit être perçue comme un investissement dont il est permis d'attendre un retour.

C) Le CH de Dreux doit s'engager dans une politique de sécurité de manière progressive et à court terme privilégier le déploiement de son SIH

a) Le niveau exceptionnel des dépenses d'investissement consacrées à l'informatique ces dernières années ne pourra être maintenu

Le CH de Dreux consacre depuis quelques années une part croissante de son budget à son informatisation. Il est cependant difficile d'évaluer de manière précise et exhaustive le montant total des dépenses consacrées au système d'information. En effet, le champ des dépenses qui peuvent y être rattachées est très large et leur recensement est donc rendu complexe. Au-delà des dépenses de matériel informatique, de logiciels, de maintenance et de consommables, il faudrait également identifier les dépenses indirectes telles que les prises informatiques nécessaires au raccordement des stations de travail au réseau, les coûts de main d'œuvre et de fournitures liées aux travaux d'adaptation des locaux tels que l'aménagement d'un nouveau local technique, etc.

Le tableau suivant recense les dépenses d'investissement et d'exploitation engendrées par le système d'information du CH de Dreux au cours de ces trois dernières années.

DEPENSES D'INVESTISSEMENT				
		2003	**2002**	**2001**
H21831	Bureautique et informatique (seulement informatique)		485 334	284 050
H21832	Matériel logiciel informatique	1 625 945		
Budget d'investissement total		6 300 242	6 155 451	8 007 101
Part du budget d'investissement consacrée aux dépenses informatiques		**25,81%**	**7,88%**	**3,55%**

DEPENSES D'EXPLOITATION				
		2003 (extrapolation sur 12 mois)	**2002**	**2001**
Charges Groupe 1	Rémunération du personnel	315 119	296 255	282 158
H615611	Maintenance informatique à caractère médical	28 580	26 850	414
H60284	Fournitures pour informatique	64 500	63 300	62210
H60641	Fournitures informatiques	13 510	10 107	123
H60643	Imprimés informatiques	4 050	3 040	1 165
H61351	Location informatique	0	0	0
H61554	Réparation de matériel informatique	820	732	812
H615618	Maintenance informatique autres	10 500	13 466	12 038
H6261	Liaisons informatiques ou spécialisées	8 030	10 967	1 518
H6284	Informatique (extérieur)	149 880	193 830	215 598
H6811283	Amortissement matériel informatique	294 418	314 041	254 747
Total des dépenses d'exploitation consacrées à l'informatique		889 407	932 589	830 783
Budget d'exploitation total		87 022 710	83 882 509	80 257 175
Part du budget d'exploitation consacrée aux dépenses informatiques		**1,02 %**	**1,11 %**	**1,03 %**

La première partie du tableau, qui retrace les dépenses d'investissement, montre l'effort fait ces dernières années pour la modernisation de l'informatique de l'établissement. Les dépenses d'investissement ont ainsi augmenté de plus de 70% entre 2001 et 2002 et de 235% entre 2002 et 2003. L'année 2003 est toutefois une année particulière, puisque plus du quart du budget d'investissement a été absorbé en 2003 pour l'achat des logiciels et des matériels destinés au remplacement complet du SIH. Une telle opération est exceptionnelle dans la vie d'un établissement. En règle générale, il est en effet toujours préférable d'opérer des modifications ponctuelles et d'effectuer une modernisation progressive plutôt que de remplacer purement et simplement l'ensemble du système. Les circonstances rappelées plus haut ont fait que cela n'a pas été possible. L'avantage de ce changement massif est sans doute l'homogénéité qui en résultera au niveau des matériels et des logiciels.

b) L'informatique du CH de Dreux a un coût de fonctionnement peu élevé

Les dépenses d'exploitation se maintiennent à un niveau relativement faible, notamment du fait de la productivité de l'équipe informatique dont les effectifs sont plus faibles que la

moyenne. Les coûts de maintenance sont en revanche élevés en valeur absolue et représentent près de 20% du budget de fonctionnement consacré à l'informatique. La part des dépenses consacrées à la maintenance des matériels et des logiciels informatiques dans l'ensemble des dépenses de maintenance de l'établissement, y compris la maintenance des équipements médicaux est de 23%, ce qui est tout de même significatif de l'importance stratégique prise par le système d'information et de son coût pour l'hôpital.

c) Les perspectives d'évolution des dépenses informatiques

D'après la DHOS, les investissements concernant les systèmes d'information représentent en moyenne 5% du total des investissements hospitaliers et les dépenses d'exploitation 1,5% des budgets des établissements publics de santé. Il est difficile de situer le CH de Dreux par rapport à cette moyenne en investissement du fait de la situation spécifique dans laquelle il se trouve en ce moment. Pour ce qui relève du budget d'exploitation, il se trouve pour le moment en deçà de la moyenne. Dans son rapport, le Professeur Fieschi rappelle qu'aux Etats-Unis, ces budgets se situent au-dessus de 3% et il recommande que ce niveau soit un objectif à atteindre dans les trois ou quatre ans pour les hôpitaux français. Il est probable que les dépenses de fonctionnement du CH de Dreux vont augmenter dans les années à venir à la suite du déploiement de nouveau matériel. La maintenance des logiciels, une fois la période de prise en charge gratuite écoulée (qui varie entre un et trois ans), représentera une masse budgétaire supérieure au coût actuel. Il est probable également que l'équipe informatique sera à nouveau amenée à se renforcer si l'organisation d'une vraie politique informatique prenant en compte la sécurité se met en place.

3.2 L'organisation de la politique de sécurité informatique

3.2.1 Au niveau décisionnel

A) Définir la politique de gestion du risque informatique

a) L'aspect stratégique de la rédaction du schéma directeur du SIH

Le projet d'établissement, orienté par le projet médical, énonce les choix stratégiques qui vont influencer la marche de l'établissement au cours des années à venir. De fait, le projet d'établissement dicte au schéma directeur les évolutions du SIH. « Le projet d'établissement définit, notamment sur la base du projet médical, les objectifs généraux de l'établissement dans le domaine médical et des soins infirmiers, de la politique sociale, des plans de formation, de la gestion et du système d'information ». Le schéma directeur

contribue au projet d'établissement, il en est une des parties. Ses orientations sont cohérentes avec celles du projet d'établissement, qui les a définies. Rien de ce qui concerne l'établissement n'est vraiment étranger au système d'information. Toutefois, les orientations majeures du schéma directeur doivent lui être dictées en priorité par le projet médical. Il est en effet normal que la raison d'être de l'hôpital, qui est de soigner, dicte ses orientations.

Le schéma directeur en vigueur au CH de Dreux reste très sommaire. Rédigé en 1999, il est uniquement consacré à l'obligation de changer le système d'information à l'horizon de juillet 2004. Il serait souhaitable qu'à l'occasion du renouvellement en cours du projet d'établissement un nouveau schéma directeur puisse être rédigé.

b) La méthode d'élaboration du schéma directeur

Le ministère de la santé préconise une méthode d'élaboration dans un ouvrage intitulé Elaboration des schémas directeurs du système d'information des établissements hospitaliers publics. Cette méthode propose six phases, qui sont les suivantes :

1) Constitution des structures de travail et recueil des orientations des principaux responsables de l'établissement
2) Analyse de l'existant et des besoins
3) Elaboration de la cible visée par l'évolution du système d'information
4) Recherche de scénarios possibles et identification de leurs points forts et de leurs points faibles
5) Production du plan d'action qui permettra d'atteindre la cible selon le scénario retenu
6) Déploiement du schéma directeur

c) La place de la politique de sécurité dans le schéma directeur

La sécurité du système d'information doit avoir sa place dans le schéma directeur. Elle peut être traitée à l'occasion de l'étude de chacun des blocs composant le système d'information, ou bien faire l'objet d'un chapitre à part, ce qui permet de bien isoler la problématique et de faire ressortir le caractère transversal de la politique de sécurité. Cette réflexion dans le cadre du schéma directeur doit permettre de préciser les attentes des différents acteurs en matière de sécurité et de confidentialité des données et de repérer les moyens qu'il est possible d'y consacrer. Elle peut être l'occasion dans un premier temps d'initier la mise en place d'une politique de sécurité, puis de suivre sa mise en place et d'évaluer ses résultats. L'implication de la Direction de l'établissement dans la définition des orientations est essentielle. La politique de sécurité doit en effet s'insérer dans la stratégie de l'établissement, être adaptée à sa culture, mais aussi doit se voir attribuer les moyens nécessaires à sa mise en œuvre.

B) Créer un Comité de sécurité du système d'information

Le Directeur peut être assisté dans sa tâche de définition des orientations de la politique de sécurité par un Comité de sécurité du système d'information. Ce Comité peut être composé des quelques acteurs les plus directement impliqués par cette politique. A titre indicatif, peuvent en faire partie le Président de la Commission médicale d'établissement, le Directeur des soins infirmiers, le responsable du Département d'information médicale, le responsable du service informatique, l'ingénieur chargé des services techniques et des travaux.

C) Faire rédiger un document de politique de sécurité et une charte de sécurité

La politique de sécurité doit obligatoirement être formalisée. Sa mise en œuvre étant nécessairement progressive, sa rédaction peut se faire en deux étapes et faire l'objet de plusieurs documents.

Dans un premier temps, un document d'orientation peut être écrit, définissant ce qu'est la sécurité de l'information, rappelant son importance à l'hôpital, ainsi que les grands principes de sécurité de l'information. De façon succincte, ce document doit aussi présenter les axes directeurs de la politique de sécurité (conformité aux exigences légales et contractuelles, protection de la confidentialité, gestion de la continuité, etc.) et définir les responsabilités relatives à la gestion de la sécurité du SIH. La direction doit approuver ce document et le publier. Il est important que les responsables de services s'en voient remettre un exemplaire et qu'une action de communication soit entreprise à l'intention de l'ensemble du personnel.

Dans un second temps, une fois les règles opérationnelles établies et validées, le Directeur pourra publier, afin de sensibiliser et de responsabiliser le personnel, une charte de sécurité reprenant les principes directeurs de la politique de sécurité et les consignes à respecter.

Ce travail de rédaction doit s'effectuer, en lien avec la Direction, par le responsable de la sécurité informatique.

3.2.2 Au niveau du pilotage

A) Situation actuelle

Le responsable de la sécurité informatique est aujourd'hui de facto le responsable du service informatique. Aucune fonction spécifique n'est définie pour accomplir cette mission précise. En pratique néanmoins, un des membres de l'équipe informatique s'est

vu confier par le responsable du service la tâche de veiller à la sécurité et de réaliser les études visant à améliorer celle-ci. Cette situation n'a pour l'instant pas posé de difficulté particulière et n'a pas conduit à négliger cet aspect dans l'exploitation et le déploiement du système d'information.

B) Nomination d'un RSSI

L'inconvénient de cette solution est qu'elle ne permet pas de donner à la sécurité la dimension stratégique qui devrait être la sienne. Aussi, il est conseillé de procéder à la nomination d'un responsable de la sécurité des systèmes d'information, dont les missions et les responsabilités feraient l'objet d'une fiche de poste et d'une délégation formelle du Directeur, avec l'attribution de moyens d'action en rapport avec les missions confiées. Le RSSI a 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. Il est le maître d'ouvrage des projets de sécurité et participe à la sensibilisation des acteurs de la sécurité. Le RSSI est rattaché fonctionnellement au Directeur général, même s'il reste rattaché hiérarchiquement au Directeur chargé des systèmes d'information.

Dans une structure telle que le CH de Dreux, doté d'une équipe informatique restreinte, cette fonction peut être occupée par le responsable du service informatique. Il s'agit donc davantage de lui attribuer des responsabilités précises en matière de sécurité que de bouleverser l'organigramme du service.

C) La politique de sécurité informatique doit s'articuler avec la démarche qualité et la gestion des risques.

La démarche de gestion du risque informatique au CH de Dreux peut s'appuyer sur l'expérience acquise en matière d'amélioration de la qualité et sur la mise en place récente d'une politique de gestion des risques.

La mise en place des structures de la politique qualité a en effet débuté dès mai 1997 et l'autoévaluation en vue du lancement de la procédure d'accréditation a eu lieu dès mai 1999, pour une visite dès mai 2000. La politique qualité repose sur un comité de pilotage comprenant vingt-sept membres représentant le corps médical, la direction et le personnel paramédical, auxquels s'ajoute le service qualité. Ce comité assure l'interface entre le terrain, les instances délibératives et consultatives et de façon générale les structures liées à la qualité et à la gestion des risques. Au niveau de la direction, le secteur de la qualité a été confié à un directeur adjoint, qui dispose d'un outil opérationnel, le service qualité, composé d'un médecin, d'un cadre supérieur de santé et d'une secrétaire. Dans les différents services de l'établissement, ont été identifiés des

référents qualité qui servent de relais à la politique qualité. La gestion du risque informatique peut donc s'appuyer sur cette organisation qui a prouvé son efficacité.

Une politique de gestion des risques s'institutionnalise elle aussi et se structure depuis une année environ. Une cellule de gestion des risques composée de huit personnes est chargée de la mise en œuvre opérationnelle de cette politique. Elle fait valider ses orientations par une commission de gestion des risques composée notamment des membres de la cellule de gestion, des référents des vigilances sanitaires, des directeurs et des représentants des instances. Si l'ingénieur des services techniques est bien membre de la commission, de même que le responsable du service de sécurité des biens et des personnes, en revanche il est regrettable qu'aucun représentant du service informatique ne le soit. Une des premières démarches de ces structures a été la mise au point d'un recueil des événements indésirables à travers une fiche de signalement qui peut utilement servir au recensement des incidents liés au système d'information. La panne informatique figure d'ailleurs sur la liste non exhaustive des événements indésirables prévus par la fiche.

3.2.3 Au niveau opérationnel

A) Identifier les responsables

La première étape d'une politique de sécurité doit être la responsabilisation du personnel vis-à-vis du patrimoine de l'établissement.

a) Définir les responsables de l'information

Toute information ou groupe d'information doit avoir un responsable désigné, qui se charge de faire appliquer la politique de sécurité pour ce groupe d'informations et qui définit dans le service dont il a la charge les règles de gestion des données. Par exemple, le directeur chargé des finances sera responsable des données financières, le médecin responsable du DIM sera chargé de la sécurité des données issues du PMSI.

b) Définir les responsables des infrastructures

L'environnement technique du système d'information est un maillon incontournable de sa sécurité. Il est donc important que la politique de sécurité définisse les responsabilités en matière de gestion du réseau électrique, du réseau téléphonique, du réseau informatique, etc. De même, certaines prestations logistiques garantissent le bon fonctionnement du système d'information. Il en va ainsi de la sécurité des biens et des personnes, des achats et de l'approvisionnement. Là encore, la politique de sécurité doit définir les responsables de ces services.

c) Définir les responsables des applications informatiques

Au sein du service informatique, la répartition des responsabilités est déjà effectuée. Chaque membre de l'équipe a la responsabilité en premier ressort de certaines applications et de certains aspects de la politique informatique. La polyvalence est cependant encouragée et le recours à un collègue est toujours possible. Ces attributions figurent dans la fiche de poste des agents.

B) Prévoir l'organisation d'audits périodiques

a) Principe de l'audit de sécurité

Le défaut de sécurité du système d'information et l'insuffisante protection de la confidentialité des données étant, comme nous l'avons vu, susceptibles d'engager la responsabilité du directeur de l'établissement en cas de sinistre ayant provoqué un dommage, celui-ci doit être périodiquement informé de la qualité de l'application de la politique de sécurité et du niveau de protection effectif.

L'organisation d'un audit interne annuel est de nature à permettre ce suivi régulier. L'audit est une étude méthodique d'une situation concernant une organisation ou des prestations, afin de mesurer les écarts entre fonctionnement normal et réel.

En matière de risque informatique, l'audit de sécurité est défini par la commission de normalisation informations de santé comme une «revue indépendante et [un] examen des enregistrements et de l'activité du système afin de vérifier l'exactitude des contrôles du système pour s'assurer de leur concordance avec la politique de sécurité établie et les procédures d'exploitation, pour détecter les infractions à la sécurité et pour recommander les modifications appropriées des contrôles, de la politique et des procédures ».

b) Déroulement de l'audit interne

L'auditeur interne doit évidemment avoir les compétences nécessaires. Etant donnée la technicité requise, il semble que seul un membre du service informatique soit à même de réaliser cet examen. Le support de cet audit doit être une norme reconnue, comme la norme ISO 17799 ou la norme ENV 12924. Les auditeurs vont établir un bilan de l'existant. L'audit interne peut aussi être l'occasion d'une analyse de l'historique des sinistres, ce qui est rarement fait jusqu'à présent, faute de temps.

c) Recours à l'audit externe

De manière plus espacée, tous les trois ou cinq ans par exemple, un audit externe effectué par un organisme privé ou public, peut permettre de confirmer les résultats obtenus en interne mais avec une charge financière assez lourde. L'avantage de l'audit

externe est de permettre la formulation des dysfonctionnements ressentis mais non reconnus par le personnel. L'auditeur va médiatiser le message et le retranscrire avec des mots qu'une direction ne pourrait peut-être pas se permettre.

3.3 Les grands axes d'action prioritaires du management de la sécurité informatique

3.3.1 Approfondir la connaissance des risques liés au SIH au sein de l'établissement

A) Analyser les risques

a) Identifier les ressources à inventorier

Les ressources du système d'information font partie des biens de l'établissement dans la mesure où elles participent à son existence, à son développement et contribuent à l'accomplissement de ses missions. On peut distinguer différents types de ressources :

- les données : bases de données, enregistrements, archives, etc.
- la documentation : documentation système, procédures d'exploitation et de maintenance, plans de continuité
- logiciels : applications, systèmes d'exploitation, etc.
- les structures supports : ordinateurs, réseaux, climatisation, onduleurs, etc.
- les ressources humaines

La valeur intrinsèque de ces ressources s'exprime d'une part par leur valeur en tant que biens marchands, d'autre part par l'évaluation de la contribution qu'elles apportent à la réalisation des missions de l'hôpital, et enfin par l'évaluation des conséquences de leur absence ou de leur dysfonctionnement.

b) Classifier les ressources

Dans la mesure où la limitation des moyens d'action impose de privilégier en priorité la sécurité des biens jugés de plus grande valeur, il est naturellement nécessaire de déterminer en quoi chaque ressource importe. Cette évaluation est l'objet de la classification des ressources.

Etablir une grille de classification des ressources

Cette classification doit être basée sur des critères d'impact sur les soins apportés aux patients, sur le respect des exigences légales, de la déontologie médicale et sur l'activité de l'établissement. La classification d'une information est en effet le critère de base qui

détermine la façon dont elle va être manipulée et protégée. Le GMSIH propose la grille suivante

Niveau	Disponibilité	Intégrité	Confidentialité
1 **faible**	**INTERRUPTION <= 3 J** Une indisponibilité temporaire est acceptable	**SIGNALEMENT** Toute perte d'intégrité doit être signalée	**PUBLIC** Les informations peuvent être lues par tous
2 **sensible**	**INTERRUPTION <= 8 H** Une indisponibilité momentanée est tolérée, mais doit être signalée et sans conséquence sur le service fourni	**SIGNALEMENT / CORRECTION** Toute perte d'intégrité doit être signalée et corrigée	**RESTREINT** Les informations sont diffusées ou accessibles par des populations identifiées et contrôlables
3 **critique**	**INTERRUPTION <= 1 H** Les informations doivent toujours être fournies pour remplir le service attendu	**JUSTIFICATION** L'information doit rester intègre durant la période d'utilisation. Toute perte en dehors de cette période doit être signalée et corrigée	**SECRET MEDICAL OU PROFESSIONNEL** Les informations sont protégées par le secret médical ou le secret professionnel et par la législation sur les données à caractère médical
4 **stratégique**	**INTERRUPTION <= 15 MIN** Les informations doivent être accessibles en permanence et utilisables par tous les services concernés	**CERTIFICATION** Les informations sont certifiées intègres pendant toute leur durée de vie ou période de validité	**HAUTE PROTECTION** Le secret médical est renforcé pendant toute la durée de vie ou période de validité

Définir les responsables de la classification

La responsabilité de la classification d'une ressource doit être attribuée à l'émetteur ou au responsable de la ressource.

c) Utiliser les méthodes communes d'analyse des risques

Prévenir les risques suppose de les connaître. La première étape de la mise en œuvre d'une politique de gestion du risque est donc la mise en évidence des événements redoutés. Deux outils peuvent être utilisés : l'analyse préliminaire des risques (APR) et l'analyse des modes de défaillance, de leur effet et de leur criticité (AMDEC)

L'APR est à la base de toute démarche de maîtrise des risques. Ses principes sont les suivants :

- identification des événements redoutés
- évaluation du niveau de risque (criticité) par la détermination de la gravité des conséquences des événements redoutés et de leur probabilité d'occurrence
- définition de mesures en réduction de risque visant à diminuer l'occurrence de l'événement redouté (mesure de prévention) et/ou à en diminuer les conséquences (mesure de protection).

La mise en œuvre de l'APR essaie de retracer le processus accidentel et constitue donc un moyen d'établir une base d'informations événementielles sur les systèmes complexes,

permettant ainsi d'envisager les événements redoutés ayant pour origine une combinaison de défaillances.

L'AMDEC a été développée dans les années soixante. Il s'agit d'une méthode très rigoureuse de recensement des défaillances potentielles et de leur impact sur le fonctionnement d'un système donné. Son objectif est de permettre l'identification et la prévention des problèmes. L'AMDEC passe par le franchissement de huit étapes successives :

1. Description du produit, du processus, etc.
2. Détermination des modes de défaillance
3. Evaluation des effets de la défaillance
4. Détermination des causes
5. Evaluation des contrôles actuels
6. Cotation de la criticité des défaillances : fréquence d'apparition, gravité, etc.
7. Fixation des actions correctives, désignation des référents concernés et lancement des actions
8. Détermination de la nouvelle criticité après mise en œuvre des actions correctives

L'intérêt de l'AMDEC est sa précision dans le recensement des défaillances potentielles et de leur impact. Cependant, la méthode présente plusieurs inconvénients. Tout d'abord, elle est lourde à mettre en œuvre. Ensuite, elle ne permet pas de prendre en compte les défaillances combinées.

Ces démarches génériques peuvent être utilisées pour la prévention des risques liés au système d'information. Elles doivent néanmoins être adaptées, ce qu'ont fait les concepteurs de méthodes spécifiques d'analyse des risques informatiques.

B) Faire le bilan de la sécurité informatique au CH de Dreux

a) Méthode choisie

Les méthodes d'analyse des risques informatiques

Il existe un certain nombre de méthodes d'analyse des risques informatiques, en particulier celles qui sont diffusées par le CLUSIF, comme MARION ou MEHARI, et de méthodes d'évaluation de la sécurité, comme la norme ISO 17799. Celles-ci permettent aux établissements d'identifier leurs risques et de quantifier les efforts à fournir en matière de sécurité du système d'information pour être conforme à la législation et aux bonnes pratiques de sécurité. Elles peuvent être adaptées à une analyse des risques en milieu hospitalier mais présentent un certain nombre d'inconvénients, dont la lourdeur de leur

mise en œuvre, qui nécessite un niveau de connaissances minimum en informatique. De ce fait, ces méthodes ne produisent des résultats qu'au terme d'un long et minutieux travail d'analyse.

Le guide d'autoévaluation du GMSIH

Le GMSIH propose depuis quelques mois un guide d'autoévaluation basé sur la norme ISO 17799, plus adapté aux besoins des établissements hospitaliers. Ce guide vise à offrir aux établissements de santé les moyens :

- d'apprécier leur niveau de maturité en termes de sécurité de l'information par rapport à la mise en place d'une politique de sécurité
- d'identifier leur niveau de risque et les menaces pesant sur le système d'information
- d'identifier les actions prioritaires à conduire afin de réduire les risques ainsi identifiés
- de construire un plan d'action pluri-annuel de mise en œuvre de la politique de sécurité.

Les avantages de ce guide

Les avantages de cette méthode sont de plusieurs ordres. Elle permet tout d'abord de pouvoir obtenir des résultats utilisables dans un délai bref et sans mobiliser des compétences introuvables dans la plupart des établissements. Elle s'appuie ensuite sur des normes reconnues au niveau international et adaptées au milieu hospitalier. Enfin, le GMSIH étant une structure regroupant une partie considérable des établissements de santé, il est probable que l'usage de ce guide est appelé à se généraliser dans les établissements.

b) Les champs couverts par l'audit

Le guide couvre l'ensemble des domaines de la sécurité informatique, y compris le volet protection de la confidentialité des données. Il insiste particulièrement sur les aspects managériaux et sur la formalisation des procédures et des politiques. La liste suivante précise les aspects pris en compte.

- la sécurité physique et la sécurité de l'environnement du système d'information
- l'exploitation informatique et la gestion des réseaux
- le contrôle d'accès logique
- le développement et la maintenance des applications et des systèmes
- la gestion de la continuité
- le respect de la réglementation interne et externe
- la politique de sécurité
- le management de la sécurité

- l'inventaire et la classification des ressources
- la sécurité et les ressources humaines

Une application réalisée sous Microsoft Excel permet la saisie des réponses aux référentiels du guide et l'exploitation rapide des résultats, présentés sous une forme directement lisible et exploitable

c) Présentation synthétique des résultats

Les réponses au questionnaire ont été renseignées avec le responsable du service informatique, sans complaisance et avec le souci de disposer de résultats fiables et utilisables à l'avenir pour définir des pistes d'amélioration. Leur exposition dans ce mémoire n'a pas pour objet de porter de jugement sur la valeur du travail effectué par le personnel du CH de Dreux, mais plutôt de contribuer à l'enrichissement de ses réflexions dans ce domaine mal connu de la majorité des hôpitaux.

Un état des lieux chiffré du niveau de maturité des principaux principes de sécurité informatique[40].

Cet état des lieux est obtenu à partir de la réponse aux cent questions contenues dans le guide, dont la réponse est affectée d'un coefficient de pondération portant sur l'efficacité de la règle de la politique de sécurité en matière de réduction du niveau de risque. Plus la note obtenue est élevée, plus la maturité est considérée importante.

La représentation graphique des résultats permet de mieux visualiser les points forts et les points faibles de l'établissement.

Une représentation graphique de ces résultats[41].

Un graphique reprend les données chiffrées du tableau ci-dessus. Plus les branches de la rosace sont éloignées du centre, plus la maturité est proche de l'excellence.

Une observation globale de ce graphique permet de remarquer que la rosace occupe environ un quart de la surface totale du cercle, ce qui situe le niveau de maturité de la politique de sécurité à un niveau assez faible. Cette faiblesse serait néanmoins à relativiser en la comparant avec les résultats obtenus par d'autres établissements. Les résultats de l'enquête mentionnée plus haut laissent à penser que le CH de Dreux ne se situe pas à un niveau inférieur à la moyenne des établissements en ce domaine. Le

[40] Voir annexe IV

[41] Voir annexe V

GMSIH semble envisager la réalisation d'une nouvelle enquête auprès de ses adhérents à partir des résultats obtenus à cette autoévaluation. Ce travail permettra de mieux situer le niveau moyen de mise en œuvre des politiques de sécurité des systèmes d'information hospitaliers.

Des points faibles se dessinent nettement. Il s'agit de la formalisation d'une politique de sécurité et de la gestion de la continuité.

Des points forts se dégagent aussi, en particulier la gestion des réseaux et l'exploitation informatique ainsi que la maintenance des matériels et logiciels.

Le niveau de couverture des risques au sein de l'établissement[42]*.*

Douze menaces génériques cohérentes pour un établissement de santé sont répertoriées sur ce graphique qui reprend les données issues de l'état des lieux et prend en compte l'impact et la potentialité des risques en fonction de la grille d'aversion aux risques ci-dessous. Plus l'aire de la rosace est grande, plus le risque lié à la menace est important et moins l'établissement est couvert contre ces risques.

Table d'aversion au risque											
	⇩	**Impact**									
⇨	*Niveau*	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Potentialité	**0**	0	0	0	0	0	0	0	0	0	0
	1	0,4	0,4	0,8	1,2	1,2	1,6	1,6	2	2,8	3,2
	2	0,4	0,4	0,8	1,2	1,2	1,6	2	2	3,2	3,2
	3	0,8	0,8	1,2	1,6	2	2	2	2,4	**3,6**	**3,6**
	4	0,8	1,2	1,4	1,6	2	2	2	2,8	**4**	**4**
	5	1,2	1,2	1,6	1,6	2	2	2,4	3,2	**4**	**4**
	6	1,2	1,2	1,6	2	2	2	2,8	**3,6**	**4**	**4**
	7	1,2	1,6	2	2	2,4	3	3,2	**3,6**	**4**	**4**
	8	1,6	1,6	2	2,4	2,8	3,2	3,2	**3,6**	**4**	**4**
	9	2	2	2,4	2,8	3,2	3,6	**3,6**	**4**	**4**	**4**
	10	2,4	2,4	3,2	3,2	3,2	3,6	**3,6**	**4**	**4**	**4**

- Gravité du risque comprise entre **3,5 et 4,0** : risque **inacceptable**
- Gravité du risque comprise entre **2,5 et 3,4** : risque **inadmissible**
- Gravité du risque comprise entre **0 et 2,4** : risque **toléré**

L'utilisation de cette grille d'aversion aux risques permet d'identifier deux risques inacceptables, qui sont l'accident physique et la perte de servitudes essentielles. L'accident physique désigne toutes les menaces de type destruction de matériel suite à un accident, telles que l'incendie, le dégât des eaux, la foudre, la tempête, etc.

[42] Voir annexe VI

La perte de servitudes essentielles désigne les menaces correspondant à l'indisponibilité temporaire ou permanente d'un service indispensable au fonctionnement du système d'information mais dont la fourniture ne dépend pas de l'établissement. Il peut s'agir par exemple de la perte d'alimentation électrique, de la défaillance de l'opérateur de télécommunications, etc.

Un risque inadmissible apparaît également, la divulgation d'informations en interne, qui correspond au cas où un personnel de l'établissement prendrait connaissance d'informations qu'il n'est pas normalement habilité à connaître, que ce soit volontaire ou non.

L'identification exhaustive des risques reste à établir

L'hôpital est une structure complexe. L'identification des risques y est très difficile en raison de la diversité des corps de métiers et de la multiplicité des interactions entre les différents acteurs. L'appréhension des processus doit donc s'opérer par une approche systémique de l'hôpital.

Cette étape de recensement des risques est une étape nécessairement longue. La vocation du système d'information étend de réaliser de manière automatisée des procédures et de mettre en lien les informations produites par différents acteurs, la cartographie des risques est nécessairement complexe. Elle doit cependant être réalisée minutieusement, puisque de la qualité de ce travail de recueil des données dépend l'efficacité des mesures de prévention, de réduction et de suivi des risques.

Ce travail ne peut être l'œuvre du seul service informatique. Il doit être réalisé avec l'ensemble des professionnels et en lien avec le service qualité. Des logiciels permettant de cartographier les processus et de relier ceux-ci entre eux existent sur le marché et peuvent représenter une aide précieuse et un gain de temps non négligeable.

C) Suivre l'évolution des risques

a) Objectifs

L'hôpital constitue pour le système d'information un environnement évolutif. Il convient donc d'évaluer périodiquement son niveau d'exposition aux risques. C'est notamment le cas de façon périodique lors de la mise en place d'un nouveau schéma directeur, mais aussi pour tenir compte des changements dans les besoins et les priorités de l'établissement dus par exemple à l'ouverture d'une nouvelle activité, ou pour prendre en compte les nouvelles menaces et les nouvelles vulnérabilités créées par l'ouverture sur un réseau externe par exemple. De manière plus générale, l'évaluation périodique doit

permettre de confirmer que les mesures de contrôle sont toujours efficaces et appropriées. Cette évaluation des risques doit se faire selon une graduation des impacts portant sur la qualité des soins, le respect de la législation, la perturbation des activités ou les coûts supportés par l'établissement.

b) Mettre en place des tableaux de bord

Un tableau de bord est un ensemble d'indicateurs de synthèse pondérés en fonction de la nature et de l'importance des risques auxquels ils se rapportent et présentés sous une forme adaptée. Le tableau de bord, en fournissant une information de synthèse, met en évidence des tendances, souligne des vulnérabilités, des faiblesses ou des insuffisances. Il n'est pas seulement un instrument de pilotage de la sécurité, mais est aussi un outil de management. La plus grande difficulté est de définir le nombre minimum d'indicateurs significatifs nécessaires et d'en assurer la mesure de la manière la plus automatique possible. Le CLUSIF propose de nombreux modèles d'indicateurs et de démarches de conception d'un tableau de bord. Il faut en règle générale :

- s'assurer de sa cohérence et réaliser une mise à jour régulière avec une fréquence en fonction de la nature des indicateurs utilisés
- organiser la remontée des informations vers les acteurs concernés suivant une procédure claire et dans une forme appropriée
- définir les valeurs limites des différents indicateurs. En dessous de la valeur minimale, le niveau de sécurité n'est pas acceptable. Au-dessus de la valeur maximale, le niveau de sécurité est surdimensionné par rapport aux exigences de la politique de sécurité.
- réaliser des indicateurs de synthèse par l'agrégation d'indicateurs de mesure de natures diverses
- sensibiliser les personnes chargées de la remontée des indicateurs de mesure

c) Choisir des indicateurs pertinents

Le tableau suivant donne quelques exemples d'indicateurs pouvant servir à la construction d'un tableau de bord de la sécurité informatique.

Formaliser les politiques de sécurité (définition des règles de bonnes pratiques, description des dispositifs de prévention, de protection, de dissuasion)	- Nombre de politiques de sécurité formalisées - Pourcentage de politiques de sécurité formalisées - Nombre de règles par politique de sécurité
Etablir un schéma directeur	- Etat d'avancement du schéma directeur - Ecart par rapport aux prévisions
Sensibiliser, former et informer le personnel	- Ratio des personnels formés par rapport à l'effectif ou par rapport aux objectifs de formation - Budget annuel consacré à la sensibilisation
Définir les règles, normes et procédures techniques à respecter	Nombre de documents de référence
Faire réaliser des audits techniques et organisationnels	- Périodicité des audits - Résultats des audits en termes de nombre de faiblesses

	majeures, moyennes ou faibles
Sécuriser les architectures réseau	- Nombre d'éléments spécifiquement dédiés à la sécurisation du réseau - Nombre de sous-réseaux
Définir une politique de maintenance de la sécurité	- Date et niveau de la dernière révision des politique de sécurité - Périodicité de leur mise à jour
Définir et tester les procédures à suivre en cas d'incident	- Nombre de procédures existantes - Pourcentage des procédures testées les six derniers mois - Bilan des tests effectués

La gestion du risque informatique ne doit pas être perçue comme la soumission de l'hôpital à une contrainte supplémentaire qui réduit la latitude décisionnelle du Directeur d'hôpital. Au contraire, intégrée dans la politique globale de gestion des risques, elle permet de mieux maîtriser le processus de décision en ayant une bonne connaissance des risques existants qui sont autant d'enjeux sur lesquels le décideur doit se positionner.

3.3.2 Faire prendre en compte cet enjeu de sécurité du SIH par la politique de gestion des ressources humaines

A) Mettre en place une gestion des emplois et des compétences adaptée à cet enjeu

a) L'importance de la gestion des emplois et des compétences

Définition de la gestion des compétences

L'hôpital apparaît comme une structure qui produit des savoirs, mais le plus souvent de manière désordonnée, mal formalisée. Les savoirs collectifs de l'établissement sont assurément inférieurs à la somme des savoirs individuels parce que les rouages de transmission sont grippés, la fluidité et l'échange mal organisés. D'où la nécessité de développer la gestion prévisionnelle des compétences. La compétence est définie par G. Malglaire, du Conservatoire national des arts et métiers, comme « un ensemble de connaissances, de capacités d'action, de comportements, structurés en fonction d'un but à atteindre, dans une situation donnée ».

En informatique, la gestion des compétences est primordiale tant il s'agit d'un domaine rapidement évolutif. La sécurité du système d'information suppose une maîtrise satisfaisante des dernières technologies et de la réglementation en vigueur. Un volet essentiel de la gestion des compétences est donc la formation continue du personnel du service informatique. Cette formation devra se prolonger par la transmission des connaissances acquises à l'ensemble de l'équipe et par la formalisation de celles-ci dans des procédures accessibles par tous. Un autre volet essentiel sera la qualité du recrutement des nouveaux agents en cas d'élargissement de l'équipe.

Mise en œuvre lors du recrutement

La majorité des sinistres en matière informatique sont dus au personnel de l'établissement, d'où l'importance particulière de la phase de recrutement. Une attention particulière doit être portée aux candidats recrutés en qualité de contractuels pour un contrat à durée déterminée et aux stagiaires.

Les postes donnant accès à des matériels informatiques sensibles ou à des données confidentielles doivent faire l'objet de fiches de postes spécifiant bien cette particularité. Dans ces cas, l'identité du candidat doit être vérifiée, la demande d'extrait du casier judiciaire effectuée avant le recrutement, et les références du candidat doivent être vérifiées, par contact auprès des précédents employeurs.

Systématiquement, pour l'ensemble des postes, un rappel des obligations en matière de secret professionnel doit être fait.

Le rôle de l'encadrement en matière de sécurité

Le rôle des cadres dans la protection de la confidentialité des données et la protection du système d'information est primordial. Ils sont en effet responsables du bon fonctionnement de leur service et à ce titre ils doivent faire respecter les bonnes pratiques et la réglementation en mettant en place une organisation adaptée. La connaissance de ces exigences suppose cependant qu'ils aient reçu une formation spécifique en matière de sécurité informatique.

b) L'importance de la sensibilisation à la sécurité

La sensibilisation à la sécurité informatique constitue un point relativement fort de l'établissement.

Une charte relative à l'utilisation de la messagerie et de l'Internet[43] a été rédigée et diffusée à l'ensemble des utilisateurs de ces services qui sont appelés à y adhérer et à la signer. Cette charte rappelle les règles et usagers en vigueur sur Internet, les risques que comporte l'utilisation de ce réseau et de la messagerie et les moyens de s'en prémunir, ainsi que les sanctions éventuelles d'un non respect des règles exposées.

Lors de l'embauche, un rappel des règles du secret professionnel est fait. Les informaticiens rappellent également régulièrement les règles de bonne pratique relatives à l'utilisation du matériel informatique lorsqu'ils sont appelés à intervenir pour effectuer une action de maintenance. Cette sensibilisation doit aussi faire l'objet de rappels périodiques

[43] Voir annexe III

par les responsables des services. Elle peut prendre plusieurs formes, par exemple un rappel des consignes, un bilan annuel des incidents de sécurité, etc.

Le personnel est formé à l'utilisation des logiciels applicatifs correspondant à son poste de travail ainsi qu'aux logiciels de bureautique si nécessaire. Une salle de formation équipée permet au personnel du service informatique de dispenser des cours régulièrement. De même, dans le cadre du plan de formation continue, des actions de formation à l'informatique sont régulièrement financées par l'hôpital depuis de nombreuses années, ce qui a permis à une grande partie des agents de développer ses connaissances.

Ces modes de formation permettent d'éviter un certain nombre d'erreurs de manipulation préjudiciables à l'intégrité et à la qualité des données.

B) Le rôle des professionnels dans le signalement des défaillances et des risques

a) Organisation de procédures formalisées de gestion et de remontée des incidents de sécurité

L'établissement doit déterminer l'organisation et les procédures formalisées de gestion et de remontée des incidents de sécurité en fonction de la gravité de ceux-ci. Il s'agit donc de fixer les types d'incidents à signaler, que ce soit une infraction à la législation, une menace virale, un mauvais fonctionnement d'un matériel ou d'un logiciel.

Il faut ensuite organiser des alertes de premier niveau afin de savoir à qui s'adresser en fonction de la menace. Ce type d'organisation est déjà en place au Centre hospitalier de Dreux grâce à l'identification de référents de premier ou second niveau.

b) Mise en œuvre de procédures de réaction aux incidents

Ce point n'est pas formalisé clairement, même si les pratiques donnent satisfaction. Il s'agit de mettre en place des procédures de réaction graduées en fonction de la gravité du risque identifié. Ces procédures doivent prévoir le cheminement décisionnel et les responsabilités en cas d'impact lors de la survenue du risque.

c) Communication sur les incidents

La communication sur les incidents signalés et sur leurs enseignements lorsque ceux-ci ont été traités est une dimension à ne pas négliger. Cette communication est destinée aux utilisateurs et à la direction de l'établissement.

Elle doit se situer à plusieurs niveaux. Elle doit d'abord porter sur l'incident ponctuel qui vient de se produire. Plus largement, il faut considérer que ce « feed back », ou retour

d'expérience, est une condition de réussite de la politique de sécurité. Ce type de communication est très utilisé dans l'industrie. La direction d'EDF communique ainsi à l'ensemble des centrales nucléaires les incidents qui se sont produits dans l'une d'elles, en France comme à l'étranger. Cette connaissance des causes et des circonstances de survenue des incidents doit permettre à l'établissement d'envisager des mesures en termes de prévention, de protection, de correction ou de réaction. Le CSIH ainsi que la commission des risques peuvent être des lieux où un bilan de la sécurité du système d'information mérite d'être établi.

C) Prévoir la mise en place d'une politique d'autorisation

a) Les contrôles d'accès logique par mot de passe

L'accès logique s'effectue au travers d'un double contrôle par mots de passe. L'utilisateur doit s'identifier deux fois, une première pour accéder au réseau et une seconde pour ouvrir une session de travail dans le système d'exploitation. En outre, pour accéder aux logiciels applicatifs, une nouvelle identification est demandée sous la forme d'un login et d'un mot de passe. Le service informatique tente de faire appliquer les recommandations de la CNIL en matière de mot de passe et dispose d'un fichier les recensant. Les mots de passe doivent respecter une taille suffisante fixée à six caractères au minimum, à huit de préférence. Ils doivent être constitués d'une succession de chiffres et de lettres sans signification et surtout sans lien avec un quelconque élément de l'environnement personnel ou professionnel susceptible d'être connu par des tiers.

b) La réflexion sur l'utilisation des techniques de biométrie

Les mots de passe offrent une protection de bonne qualité s'ils répondent à ces caractéristiques, mais présentent des insuffisances encore difficiles à combler à l'heure actuelle. La diffusion des mots de passe n'est pas rare. Il est estimé que 40% des utilisateurs divulguent leur mot de passe à une ou plusieurs personnes. Se pose par exemple le problème des utilisateurs multiples d'une même station de travail. Comment assurer la traçabilité de ces accès ?

La biométrie répond en grande partie à ces questions. Depuis 1997, cette nouvelle technique est en plein essor. Le mot « biométrie » utilisé dans le domaine de la sécurité est une traduction de l'anglais « biometrics » qui correspond en fait à notre mot anthropométrie. La biométrie est basée sur l'analyse de données liées à l'individu et peut être classée en trois grandes catégories : l'analyse basée sur l'analyse morphologique (empreinte digitale, forme de la main, traits du visages, iris de l'œil, voix, etc.), l'analyse de traces biologiques (sang, salive, odeur, etc.) et l'analyse basée sur le comportement

(frappe sur un clavier d'ordinateur, dynamique du tracé de signature). La biométrie suppose à la fois la transmission des données physiques concernant des individus, mais aussi leur stockage, de sorte que si la biométrie peut sécuriser un accès ou un échange, la contrepartie sera une aliénation de liberté. La CNIL a consacré une partie importante de son 22e rapport annuel d'activité, présenté le 10 juillet 2002, à ces technologies. D'après sa doctrine, les technologies de reconnaissance biométriques ne reposant pas sur le stockage des gabarits dans une base de données centralisée ne soulèvent pas de difficulté particulière, dès lors que le gabarit est conservé sur soi, par exemple sur une carte à puce, ou sur un appareil dont on a l'usage exclusif, comme un ordinateur.

c) Un exemple de mise en place d'une véritable politique d'autorisation

Le GMSIH conseille aux établissements de mettre en place une politique de gestion des autorisations. Une autorisation est, selon la définition de la norme ISO 7498-2, « l'attribution de droits, comprenant la permission d'accès sur la base de droits d'accès ». Une politique d'autorisation s'appuie, pour autoriser l'accès à des ressources, sur des habilitations, qui sont des « droits accordés à des individus d'accéder à des informations dont le niveau de sécurité est inférieur ou égal à un niveau déterminé[44] ».

Cette politique d'autorisation doit garantir l'imputabilité des opérations à leurs auteurs via l'attribution d'autorisations à des personnes nommément identifiées dans le système d'information, permettre l'harmonisation de la gestion des autorisations pour toutes les activités de l'établissement, amener de la rigueur dans l'attribution et la révocation des autorisations et assurer une meilleure protection des accès lors de l'ouverture du SIH sur d'autres systèmes d'information.

Peu d'établissements ont mis en place une telle politique. C'est cependant le cas des Hôpitaux universitaires de Strasbourg où la politique de sécurité informatique repose largement sur le contrôle d'accès au SIH. Les droits d'accès ont été définis par les chefs de service en fonction de la légitimité a priori de cet accès, qui repose sur l'intérêt direct du malade. Le modèle retenu est basé sur la fonction de l'utilisateur et son l'affectation à un service, ce qui permet de restreindre l'accès du professionnel au dossier des patients d'un service. D'autres accès sont possibles, mais dans ce cas, la responsabilité de l'agent est maximale, puisque l'accès est alors signé puis audité. L'accès laisse une trace et devient irréfutable. Les Hôpitaux universitaires de Strasbourg ont mis en place un serveur de sécurité gérant l'ensemble des habilitations et utilisent pour ces contrôles d'accès la CPS. Ces solutions ont un coût élevé mais permettent aussi d'améliorer l'ergonomie

[44] ISO/IEC IS 2382-8 (1998) AFNOR, Commission de normalisation informations de santé

d'utilisation en rendant possible l'accès à l'ensemble des applications autorisées par un seul mot de passe, selon la technique de SSO (Single sign on).

La nécessité d'une politique comme celle-ci ne s'est pas encore fait sentir au CH de Dreux puisqu'il n'existe pas encore de dossier du patient informatisé, qui est la vraie raison d'être de cette politique de gestion des autorisations. L'attribution de droits d'accès en fonction de l'utilisateur n'est cependant pas complètement inconnue car le personnel administratif se voit déjà attribuer des droits d'accès aux données limités selon sa fonction.

3.3.3 Orienter davantage l'exploitation et la maintenance du SIH vers une plus grande formalisation de procédures de sécurité afin de garantir une continuité de fonctionnement

A) Obtenir la garantie d'une continuité de fonctionnement

a) S'assurer de la qualité des biens fournis en interne et en externe

Il est important de s'assurer du bon fonctionnement des logiciels gérant les données du SIH. Aujourd'hui encore, trop de logiciels sont mis en circulation sans avoir été suffisamment testés au préalable, ce qui peut avoir des conséquences dommageables pour la sécurité des informations, en particulier celles des patients. Des projets de normes d'évaluation des logiciels médicaux sont à l'étude dans le cadre du Comité technique du CEN. Ils pourraient comporter non seulement des normes de rédaction des programmes inspirées de celles existantes pour l'ensemble du secteur informatique (normes ISO 9002), mais également des procédures de validation de terrain du logiciel, à l'image de celles exigées pour la mise sur le marché des dispositifs médicaux et des médicaments. Les logiciels qui satisferaient à ces normes d'évaluation pourraient alors bénéficier d'une accréditation.

b) Permettre une continuité de gestion

Les établissements publics de santé assurent le service public hospitalier, ce qui les contraint à assurer une permanence de soins et les amène à devoir gérer des situations d'urgence. Le personnel des hôpitaux est amené à prévoir des situations de crise. La réglementation les oblige ainsi à prévoir l'organisation d'un plan d'afflux de victimes à l'hôpital (plan AVH) ou du Plan blanc. Malgré leur expérience, il est conseillé aux établissements de prévoir la situation d'un grave sinistre touchant le SIH.

Le CH de Dreux ne dispose pas de tels plans. Il est possible pour en élaborer de s'inspirer des principes méthodologiques pour la gestion des risques en établissement de santé diffusés par l'ANAES. Les étapes suivantes doivent inspirer les réflexions.

Il s'agit en premier lieu autant que possible d'anticiper la crise. La réflexion au moment critique ne peut se développer efficacement que s'il y a eu préparation profonde des systèmes et des hommes. Le plan de gestion de crise est un outil indispensable parce qu'il fixe des règles d'intervention et allège considérablement le travail de base au moment d'une crise. Ce plan définit ce qui est à faire lors de la survenue d'une crise. Il permet aussi de réaliser des simulations qui favorisent l'apprentissage des acteurs. Identifier la crise le plus tôt possible permet d'en limiter l'impact. Il s'agit pour cela d'avoir une attitude de veille, de savoir identifier les signaux faibles, notamment grâce aux tableaux de bord.

En second lieu, il faut se préparer à gérer la crise, et pour ce faire de constituer une équipe spécialisée. Le travail à conduire ne peut l'être que par un nombre réduit de personnes, d'autant que l'organisation doit continuer de fonctionner. La composition de l'équipe en charge de gérer la crise doit être connue. Une structure de pilotage intégrant la direction générale ainsi que les directeurs adjoints et les responsables techniques impliqués doit exister. Cette structure doit piloter les actions de prévention des risques et de réaction à la survenue des risques en mettant en place des plans de secours. En situation de crise, une structure de réaction rapide en situation de crise doit être pré-identifiée afin d'organiser les réactions appropriées. La gestion de la crise nécessite la compréhension de la situation et la définition d'une réponse adaptée. Le repérage préalable des secteurs à risque permet de s'organiser de façon à disposer des informations utiles à l'action lorsque le risque survient. La qualité de l'organisation de l'établissement se révèle dans les situations de crise. La préexistence d'une démarche qualité est un facteur favorisant car la confiance et la délégation accordées aux individus et aux équipes dans le fonctionnement normal de l'institution permettent au moment du sinistre aux acteurs de prendre les initiatives adaptées.

En troisième lieu, il est conseillé de communiquer sur la crise. La communication doit être conduite de façon centralisée et dirigée à la fois vers le personnel de l'établissement afin d'assurer la cohésion de sa propre organisation, vers les éventuelles victimes et leurs familles, vers les autorités de tutelle et vers le public et les médias.

c) Elaborer des plans de continuité

Le plan de secours informatique permet selon les situations de crise envisagées de répondre aux exigences fonctionnelles de sécurité déterminées et validées par

l'établissement en matière de délai maximal d'interruption totale et de pertes de données maximales autorisées. La mise en place d'un projet de plan de secours informatique s'effectue sous la direction de la structure de pilotage. Le plan de secours informatique doit avoir été rédigé de manière exhaustive mais compréhensible par un personnel soumis à un environnement de crise. Il doit être stocké de manière sûre afin d'être accessible à n'importe quel moment.
En parallèle, l'établissement doit prévoir un plan de secours des ressources stratégiques non informatiques. Ces deux plans sont en effet complémentaires dans la mesure où un sinistre important risque d'avoir des impacts qui dépassent largement le seul système d'information. Ce plan de secours de ressources non informatiques doit permettre une reprise de l'activité dans des conditions conformes aux exigences fonctionnelles de continuité en matière de locaux, d'infrastructures ou de services logistiques.

L'établissement doit mettre en œuvre les moyens permettant d'utiliser le plan de continuité à tout moment. Les procédures de mise à jour des différents éléments le composant doivent avoir été prévues dès leur conception et être appliquées. Cela concerne en premier lieu le changement des acteurs ou de leurs coordonnées, mais également le changement des contrats ou de la législation. Des astreintes du personnel du service informatique devront avoir été organisées, ce qui n'est pas encore le cas. Aujourd'hui, en cas de dysfonctionnement, les appels se font sans procédure écrite ni cadre réglementaire et reposent donc sur le bon vouloir des informaticiens. Le maintien en conditions opérationnelles doit être assuré par des plans de tests qui, effectués régulièrement, permettent de valider et d'améliorer une mise en œuvre. Il s'agit de prévoir des tests variés en terme d'ampleur et de mode de déclenchement. Certains peuvent ainsi être préparés à l'avance, d'autres avoir lieu de manière inopinée. Chaque fin de test doit permettre d'obtenir un bilan détaillé et un plan d'action à mener rapidement sur le plan de secours. Les résultats des tests doivent impérativement transmis à l'ensemble des intervenants.

B) Poursuivre la modernisation du SIH

a) Sécuriser le matériel

De nouveaux serveurs sécurisés ont été acquis par le CH en août 2003. Alors qu'actuellement il existe un serveur par service, le but est de centraliser les serveurs d'applications et de sauvegarde.

Ces deux nouveaux serveurs disposent d'une double alimentation et d'une double ventilation, ainsi que d'une batterie de secours afin de pallier une éventuelle défaillance de l'alimentation électrique. En cas de problème électrique, un onduleur intégré – qui vient

en supplément de l'onduleur de l'hôpital - permet le déclenchement programmé d'un arrêt « propre » du système.

La sécurité physique de ces matériels est également prévue puisque chacun des serveurs va se trouver dans un local technique différent. Aujourd'hui, il n'existe en effet qu'un seul local technique, situé au rez-de-chaussée inférieur du bâtiment principal. Un deuxième est en cours d'aménagement, qui va se situer à l'extérieur du bâtiment, à une distance d'environ cent mètres du premier. Les deux locaux disposeront de détecteurs d'incendie et de capteurs de température avec répétition d'alarme au poste de sécurité de l'hôpital.

b) Sécuriser les données

Les disques de données sont eux aussi sécurisés par la mise en œuvre de la technologie RAID 1, recommandée par Oracle dont le SGBD génère beaucoup d'écritures. Cette technique a pour but de dupliquer l'information à stocker sur plusieurs disques, en miroir. On obtient ainsi une plus grande sécurité des données, car si l'un des disques tombe en panne, les données sont sauvegardées sur l'autre. De plus, étant donné que chaque disque possède son propre contrôleur, même lorsque l'un tombe en panne, le serveur peut continuer à fonctionner. Cette technologie est cependant onéreuse car seule la moitié de la capacité de stockage est utilisée. Le second serveur, servant de sauvegarde, est équipé d'un logiciel permettant la surveillance automatique des incidents pouvant survenir dans l'exploitation des systèmes et le basculement automatique, en cas de problème, des ressources d'un système sur l'autre. Ainsi, si un serveur connaît une défaillance, l'exploitation se poursuit sur l'autre et seule la transaction en cours est perdue par l'utilisateur.

La sécurité du réseau doit cependant être encore renforcée. En effet, pour l'heure le routeur situé au cœur du réseau est unique et non secouru. La mise en place d'un second routeur permettrait de découper le réseau en deux étoiles distinctes qui desserviraient deux parties distinctes du réseau mais pourraient se secourir en cas de problème. Ce second routeur bénéficierait en outre d'une technologie permettant un transfert de données plus rapide, à 1 Gbit, dont il est envisageable de faire bénéficier les applications prioritaires comme le dossier médical.

c) Optimiser le système de sauvegarde

L'achat des deux serveurs permet la mise en place d'un SAN, c'est-à-dire d'un réseau de stockage. Le SAN est un système de sauvegarde partagé installé sur un réseau indépendant du LAN. Avec cette technique, la gestion physique des données est séparée de la gestion des serveurs applicatifs de l'établissement, ce qui permet de faciliter l'administration en la centralisant sur un seul serveur, d'améliorer le niveau de sécurité

des données en l'effectuant sur une architecture à haute disponibilité et de garantir l'évolutivité par simple connexion de nouveaux équipements au réseau.

Il s'agit d'une technique relativement coûteuse, mais dont le prix a récemment diminué. De plus, il faut considérer que, en étant partagés, les espaces de stockage sont optimisés pour assurer de meilleurs taux de remplissage des disques.
Cette technique permet d'envisager à terme une sauvegarde automatisée des fichiers réalisés sur les applications bureautiques, ce qui n'est actuellement pas encore le cas.

Les solutions proposées n'ont pas d'autre ambition que de préparer le CH de Dreux aux enjeux à venir en matière de déploiement des techniques de l'information dans le domaine de la santé. Les besoins actuels se situent plus au niveau du management qu'au niveau de la technique car dans un système complexe comme le système d'information d'un hôpital, les risques se situent au niveau des interfaces et de l'organisation. Il reste donc à formaliser les procédures actuelles, à en rédiger d'autres et surtout à définir les grandes orientations d'une politique de sécurité. Celle-ci devra prévoir une mise en place progressive au fur et à mesure de l'accroissement du niveau de risque tel qu'il sera évalué régulièrement.

CONCLUSION

Dans un passage célèbre de *La phénoménologie de l'Esprit*, Hegel montre à travers la dialectique du maître et de l'esclave que l'humanité de l'homme passe par le risque. Il donne cependant raison à l'esclave qui, par le travail, acquiert la véritable maîtrise de ce risque. Ainsi, la valeur du risque est dans la mesure, la juste proportion. La morale du risque est une morale de l'équilibre.

De même, la sécurisation des données et la protection de la confidentialité des informations à l'hôpital, si elle doit ne pas être négligée, ne doit pas viser le risque zéro, qui est inatteignable et risque d'engendrer des coûts démesurés au regard de la réalité de la menace. La sécurité est actuellement un thème à la mode. Il semble qu'il faille se méfier des discours marketing souvent à la fois alarmistes et générateurs de promesses, au risque de conduire à terme à un surinvestissement dans ce domaine.

Ceci posé, ce volet de la gestion des risques à l'hôpital ne peut pas être oublié par les dirigeants hospitaliers tant son rôle dans la prise en charge des patients va devenir stratégique.

Les dernières décennies ont en effet la médecine devenir très technique, se fragmenter en de nombreuses spécialités, et l'hôpital s'industrialiser. Les conséquences de cette évolution des pratiques est la perte de vision globale de l'état de santé des malades par les professionnels, qui peut entraîner quelquefois des erreurs médicales et s'accompagne généralement de surcoûts pour notre système de santé. Les nouvelles technologies de l'information offrent aujourd'hui des moyens d'améliorer la prise en charge des patients en favorisant la coordination des professionnels de santé. Le partage des données par le biais d'un dossier du patient informatisé commun à l'ensemble des professionnels de santé et donnant au patient la possibilité d'être un des acteurs de sa santé, l'accès facilité à la connaissance, la facilitation de la coopération entre professionnels de santé grâce à la télémedecine ou la téléexpertise, sont autant de perspectives d'amélioration du fonctionnement de notre système sanitaire. Le Directeur d'hôpital, qui a pour mission de contribuer au développement de la santé publique ne peut faire l'économie d'une réflexion sur ces thèmes qui seront probablement demain des enjeux stratégiques importants. Il ne faut cependant pas perdre de vue que ces technologies ne peuvent être déployées sans la mise en place de moyens de sécurité suffisants pour protéger les données. La confiance des patients comme des professionnels est en effet une condition nécessaire au partage des données de santé. Un établissement ne peut pas prendre le risque de

constituer le maillon faible d'un réseau d'échange comme celui qui se mettra probablement en place dans les années à venir.

La prise en compte du risque informatique présente aussi pour les dirigeants hospitaliers un intérêt au niveau de la gestion des établissements. Comme toute politique de gestion des risques, la politique de sécurité informatique est l'occasion pour le Directeur d'approfondir sa connaissance de l'organisation de l'hôpital et constitue un outil intéressant d'aide à la décision. Elle est aussi le moyen de protéger un patrimoine informationnel qui devient précieux et dont la valeur financière est considérable. Les données circulant dans un système d'information hospitalier sont triplement sensibles. Elles le sont tout d'abord au niveau de la vie privée des personnes concernées, qui est potentiellement atteinte en cas de non respect de leur confidentialité. Elles le sont ensuite au niveau des conséquences qui peuvent résulter de leur manque d'intégrité ou de leur non disponibilité sur la prise en charge du malade. Elles le sont enfin en raison de la valeur économique attribuée par les financeurs de l'hôpital aux données d'activité.

Le Centre hospitalier de Dreux doit donc profiter du changement de son système d'information, dont il n'a pas choisi librement la date, pour se préparer à ces enjeux.

Bibliographie

I. OUVRAGES

AFNOR, *Catégorisation et protection des systèmes d'information de santé*, norme XP ENV 12924, avril 2000

ANAES, Manuel d'accréditation des établissements de santé, Paris : juin 2003

ANAES, *Principes méthodologiques pour la gestion des risques en établissement de santé*, Paris : 2003

BENANTEUR Y., ROLLINGER R., SAILLOUR J.-L., *Organisation logistique et technique à l'hôpital*. Rennes : Editions ENSP, 2000. 190 p.

BEUSCART R., *Rapport au Premier Ministre sur les enjeux de la société de l'information dans le domaine de santé*, 1998

CLAVIEZ J., *Sécurité informatique, sécurité des systèmes d'information et sécurité Internet*. Ste Agathe (Québec) : Editions J.C.I. inc., 2002. 192 p.

CLUSIF, *Etude et statistiques sur la sinistralité informatique en France*, 2002

DEMARNE P., ROUQUEROL M., *Les ordinateurs*, Paris : PUF, 1998. 126 p. Que sais-je ?

DUPONT M. , ESPER C., PAIRE, C., *Droit hospitalier*, Paris : Dalloz, 2001. 472 p., Cours

DUSSERRE L., DURCOT H., ALLAERT F.-A., L'*information médicale, l'ordinateur et la loi*. Paris : Lavoisier, 1999, 256 p.

FAUGEROLAS P., *Le Directeur d'hôpital face aux juges*, Paris : Ellipses, 1998. 158 p., Les professions de santé face à la justice

FIESCHI M., *Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins*, 2003. Rapport au ministre de la santé, de la famille et des personnes handicapées

FIGLAREK C., *L'utilisation de la cryptographie dans les échanges de données médico-sociales*, Rennes : ENSP, 2000, Mémoire d'élève-directeur d'hôpital

GALLET C., TOUREILLES J.-M., Histoire illustrée de 20 ans d'informatique hospitalière, Paris : 1993, 270 p.

GMSIH, *Politique de Sécurité des systèmes d'information des établissements de santé*, 2003

HOLLNAGEL E. *Human reliability analysis. Context and control*. London : Academic Press, 1993

LAGADEC P. *Ruptures créatrices*. Paris : Editions d'organisation, 2000

LE BRETON D. *La sociologie du risque*. Paris : Presses universitaires de France, 1995

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

LEOPOLD E., LHOSTE S., *La sécurité informatique*. Paris : PUF, 1999. 128 p. Que sais-je ?

LUCAS A., DEVEZE J., FRAYSSINET J., *Droit de l'informatique et de l'Internet*. Paris : PUF, 2001. 754 p., Thémis Droit privé

MATHELOT P., *L'informatique*, Paris : PUF, 1998. 127 p. Que sais-je ?

PONCON G., *Le management du système d'information hospitalier*. Rennes : Editions ENSP, 2000. 254 p.

POUILLART A., *L'hôpital face aux risques techniques : prévenir les situations de crise*, Rennes : ENSP 1999, Mémoire d'élève-directeur d'hôpital

REASON J. *L'erreur humaine*. Paris : Presses universitaires de France, 1993

II. PERIODIQUES

AMALBERTI R., PIBAROT M.-L. *La sécurité du patient revisitée avec un regard systémique*. Gestions hospitalières, janvier 2003, n°421, pp 18-37

BOSSI J. *Les réseaux de santé et la gestion du dossier médical sur Internet : les garanties de la loi informatique et libertés*. Actualités Jurisanté, mars / avril 2003, pp. 21-23

BOUTE C., HAMMELIN C., LEFEVRE M., *Protection des informations du patient. Exemple de la cellule Confidentialité du CH de Laval*. Gestions hospitalières, mai 2003, n°425, pp 392-396

CHARBONNEAU C. *Le dossier médical électronique*. Actualités Jurisanté, mars / avril 2003, n°41, pp.4-9

ESPER C. *Réseaux de santé et circulation électronique des données. Questions de droit*. Actualités Jurisanté, mars / avril 2003, pp. 16-20

LONGEON R. *Pour une approche systémique de la sécurité.* Sécurité informatique, février 2001, n°33, pp. 1-3

LONGEON R., BOUVIER P. *Le tableau de bord de la sécurité du système d'information.* Sécurité informatique, juin 2003, n°45, pp. 1-6

ROUAULT B. La gestion des risques techniques à l'hôpital. Techniques hospitalières, avril 1998, n°625, pp 35-38

SEGADE J.-P., PONTIES O. *Une charte informatique dans un CH, pour quoi faire ?* Gestions hospitalières, novembre 2002, n°419, pp. 712-714

SOLOVY A. *The big payback : survey shows a healthy return on investment for the info tech*. Hospitals & Health Networks, juillet 2001, pp 40-50

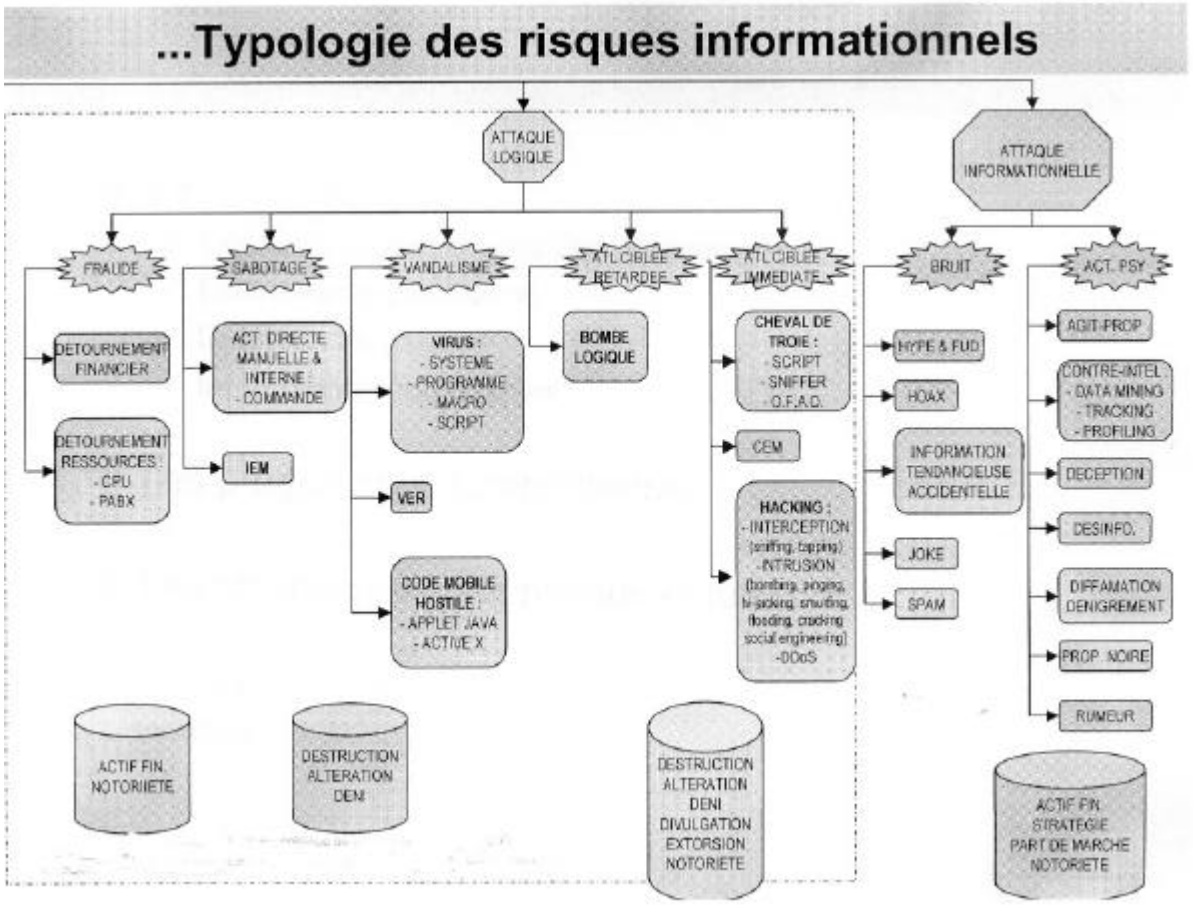
VIVET S., VILLALON A. *Le tiers hébergeur et le service de conservation de dossiers de santé accessible à distance*. Actualités Jurisanté, mars / avril 2003, pp. 12-15

III. SITES WEB

Action de l'Etat pour le développement de la société de l'information : www.Internet.gouv.fr
CERT : www.cert.org
CERTA : www.certa.ssi.gouv.fr
CIGREF : www.cigref.fr
CLUSIF : www.clusif.asso.fr
CNIL : www.cnil.fr
Computer security institute : www.gocsi.com
Conseil de l'Europe : www.coe.int
GMSIH : www.gemsih.fr
OCDE : www.ocde.org
Riskwatch : www.riskwatch.com/
SSI : www.ssi.gouv.fr

Liste des annexes

I. Typologie des risques informationnels (document CLUSIF)



II. Organisation du service informatique

	Responsable service informatique	Chef de projets	Informaticien 1	Informaticien 2	Informaticien 3	Informaticien 4
GAM		**GAM**	**GAM**	**GAM**		
GEF	GEF		**GEF**	GEF		
GRH	**GRH**		**GRH**			
Paye	**Paye**		Paye			
Laboratoire	Laboratoire					**Laboratoire**
Pharmacie			**Pharmacie**	Pharmacie		
Imagerie médicale			**Imagerie médicale**	Imagerie médicale		
GUS		**GUS**	GUS	GUS	GUS	
Cde repas. diet			**Cde repas. diet**	Cde repas. diet		
Planning ARTT	Planning ARTT	**Planning ARTT**	Planning ARTT		Planning ARTT	
GM dossier médical		**GM dossier médical**			GM dossier médical	GM dossier médical
GM dossier psy		**GM dossier psy**			GM dossier psy	
GM dossier anapath		**GM dossier anapath**			GM dossier anapath	
SAMU		**SAMU**			SAMU	SAMU
GM Urgences	GM Urgences	**GM Urgences**			GM Urgences	GM Urgences
Mater		**Mater**			Mater	
Secrétariat médical		**Secrétariat médical**				Secrétariat médical
Ateliers				Ateliers		**Ateliers**
Magasins			**Magasins**	Magasins		
Cuisines			**Cuisines**	Cuisines		
Lingerie			**Lingerie**	Lingerie		
Formation	**Formation**	Formation	Formation		Formation	
Admin.SGBD	Admin.SGBD	**Admin.SGBD**	Admin.SGBD			
Sécurité			**Sécurité**		Sécurité	
Bureautique		Bureautique	Bureautique	Bureautique	**Bureautique**	Bureautique
Gestion du parc				Gestion du parc	Gestion du parc	**Gestion du parc**
Nouvelles Technologies				**Nouvelles Technologies**	Nouvelles Technologies	Nouvelles Technologies
Réseau physique				Réseau physique		**Réseau physique**
Réseau logique				**Réseau logique**		Réseau logique

En noir : référents de premier niveau

III. Charte d'utilisation de la messagerie et de l'Internet

I. Objet
Cette charte décrit les droits et obligations de l'utilisateur d'Internet à l'hôpital de Dreux. Un agent de l'hôpital est habilité à utiliser Internet après avoir lu et approuvé cette charte qui lui a été remise.

II. Finalité d'Internet
L'hôpital de Dreux souhaite faire bénéficier ses agents des services d'Internet en rapport direct avec leur activité professionnelle. Ces services sont essentiellement : la messagerie, l'accès aux bases de connaissances et la participation à des forums.

III. Adhésion à la charte
Seuls les personnes ayant accepté cette charte en la signant sont habilitées à utiliser les services d'Internet

IV. Mot de passe
Les termes d'utilisateur ou d'Internaute, mentionnés dans ce contrat, désignent l'agent hospitalier disposant d'un équipement informatique et d'un accès Internet.

L'utilisateur s'identifie à sa machine par un mot de passe. Celui-ci est personnel et strictement confidentiel. A la demande de l'utilisateur, le mot de passe peut être modifié par le service informatique. L'utilisateur est strictement responsable de son mot de passe. Il s'engage à ne pas le communiquer sous quelque forme que ce soit et à en conserver le secret. Toute tentative d'usurpation de mot de passe d'un autre utilisateur est interdite.

V. Règles et usages en vigueur sur Internet
L'abonné a été informé de l'existence de règles et usages en vigueur sur Internet dont la violation peut amener à des sanctions de l'intervenant.

Ces règles sont connues sous le nom de « Netiquette » et sont accessibles sur Internet.

VI. Accès aux différents services
L'hôpital de Dreux s'est équipé d'outils performants permettant à la fois une bonne gestion des accès au réseau et de collecter les informations relatives à l'utilisation d'Internet. Ces informations permettent d'identifier l'ordinateur, l'utilisateur et les sites Internet accédés par celui-ci. L'internaute donne son consentement exprès afin de permettre l'utilisation de ces statistiques, et par conséquent la mise en œuvre de mesures techniques ou d'une organisation appropriée.

VII. Avertissement
L'internaute est informé des risques particuliers liés aux spécificités d'Internet. Des informations personnelles peuvent être captées et transférées, notamment dans des pays où la loi n'assure pas la protection de la personne.

Des « cookies », fichiers informatiques de suivi, peuvent également être placés à l'insu de l'internaute sur son disque dur. L'utilisateur de l'ôpital s'engage à ne pas modifier les caractéristiques des navigateurs « Internet Explorer » et « Netscape Navigator », correctement paramétrés par l'équipe informatique de l'hôpital de Dreux.

VIII. Disponibilité du service
L'hôpital met à disposition Internet d'une manière permanente, mais se réserve la possibilité d'interrompre le service, notamment pour des raisons de maintenance technique mais également en cas d'utilisation déraisonnable ou d'attaque virale externe. L'hôpital ne pourrait être tenu responsable de ces interruptions et de ces conséquences : perte d'e-mail, etc.

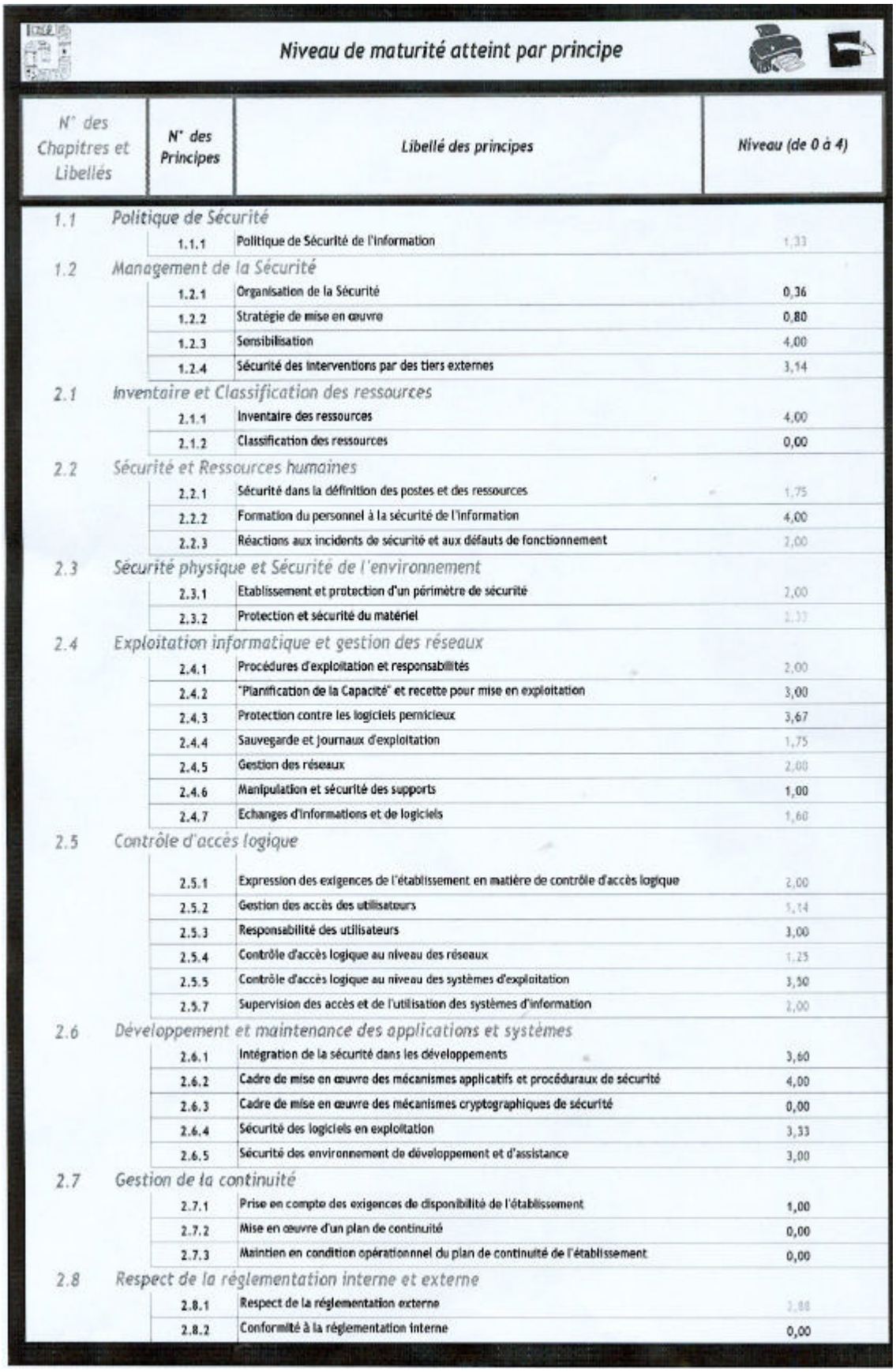
IX. Non-respect de la charte
En cas de non respect des clauses de la présente charte, la Direction de l'hôpital se réserve le droit de supprimer à l'agent l'accès aux services d'Internet et d'engager des poursuites, indépendamment des sanctions administratives vis-à-vis de toute personne atant directement ou indirectement participé à la violation de la présente charte.

Je soussigné, Nom_____ Prénom_____

Service _____ déclare avoir pris connaissance de l'ensemble de la charte, en avoir compris les termes et m'engager à les respecter.

Fait à Dreux, le _____ **Signature**

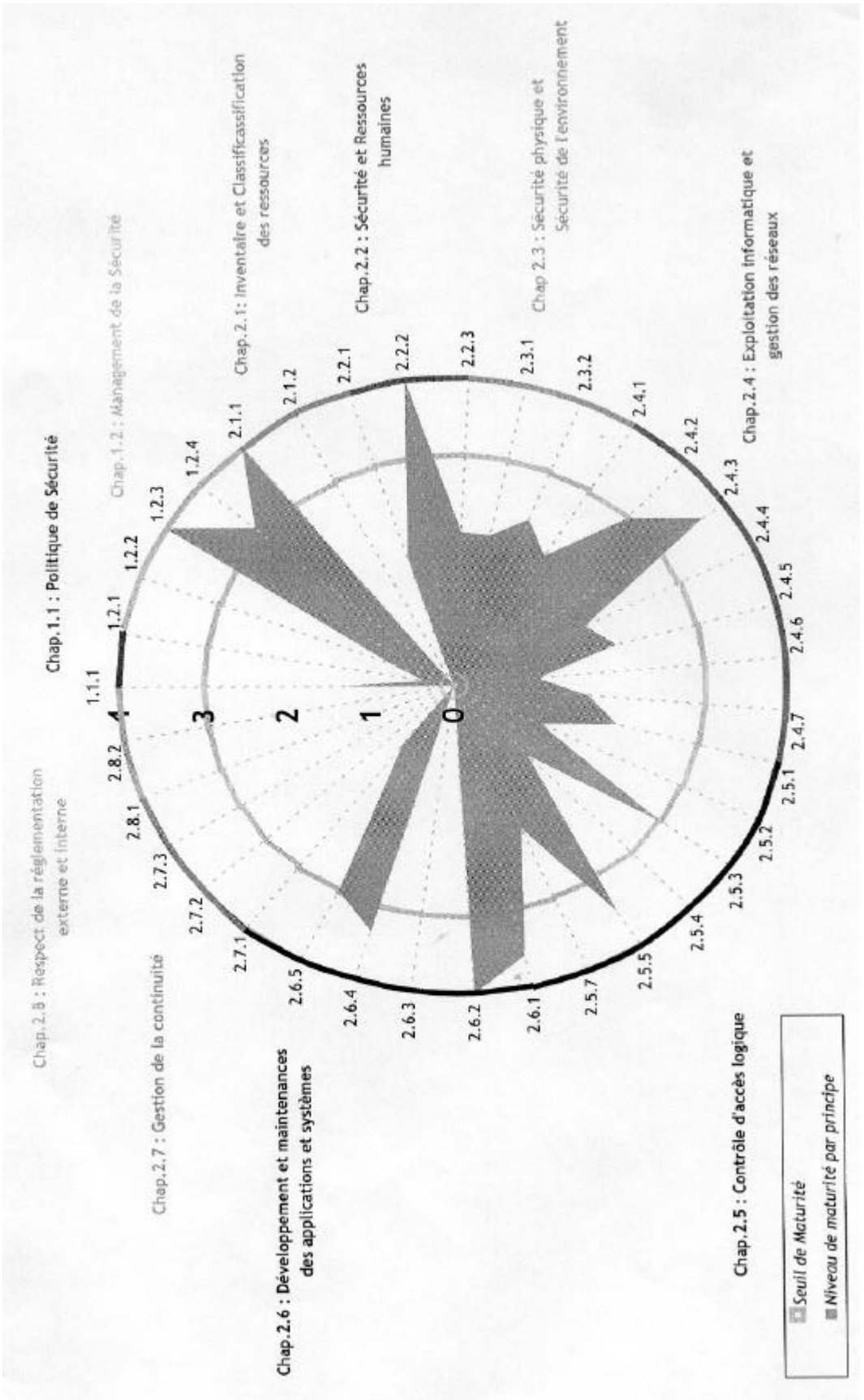
IV. Autoévaluation : état des lieux, résultats chiffrés (logiciel du GMSIH)



Niveau de maturité atteint par principe

N° des Chapitres et Libellés	N° des Principes	Libellé des principes	Niveau (de 0 à 4)
1.1		Politique de Sécurité	
	1.1.1	Politique de Sécurité de l'information	1,33
1.2		Management de la Sécurité	
	1.2.1	Organisation de la Sécurité	0,36
	1.2.2	Stratégie de mise en œuvre	0,80
	1.2.3	Sensibilisation	4,00
	1.2.4	Sécurité des interventions par des tiers externes	3,14
2.1		Inventaire et Classification des ressources	
	2.1.1	Inventaire des ressources	4,00
	2.1.2	Classification des ressources	0,00
2.2		Sécurité et Ressources humaines	
	2.2.1	Sécurité dans la définition des postes et des ressources	1,75
	2.2.2	Formation du personnel à la sécurité de l'information	4,00
	2.2.3	Réactions aux incidents de sécurité et aux défauts de fonctionnement	2,00
2.3		Sécurité physique et Sécurité de l'environnement	
	2.3.1	Etablissement et protection d'un périmètre de sécurité	2,00
	2.3.2	Protection et sécurité du matériel	2,33
2.4		Exploitation informatique et gestion des réseaux	
	2.4.1	Procédures d'exploitation et responsabilités	2,00
	2.4.2	"Planification de la Capacité" et recette pour mise en exploitation	3,00
	2.4.3	Protection contre les logiciels pernicieux	3,67
	2.4.4	Sauvegarde et journaux d'exploitation	1,75
	2.4.5	Gestion des réseaux	2,00
	2.4.6	Manipulation et sécurité des supports	1,00
	2.4.7	Echanges d'informations et de logiciels	1,60
2.5		Contrôle d'accès logique	
	2.5.1	Expression des exigences de l'établissement en matière de contrôle d'accès logique	2,00
	2.5.2	Gestion des accès des utilisateurs	1,14
	2.5.3	Responsabilité des utilisateurs	3,00
	2.5.4	Contrôle d'accès logique au niveau des réseaux	1,25
	2.5.5	Contrôle d'accès logique au niveau des systèmes d'exploitation	3,50
	2.5.7	Supervision des accès et de l'utilisation des systèmes d'information	2,00
2.6		Développement et maintenance des applications et systèmes	
	2.6.1	Intégration de la sécurité dans les développements	3,60
	2.6.2	Cadre de mise en œuvre des mécanismes applicatifs et procéduraux de sécurité	4,00
	2.6.3	Cadre de mise en œuvre des mécanismes cryptographiques de sécurité	0,00
	2.6.4	Sécurité des logiciels en exploitation	3,33
	2.6.5	Sécurité des environnement de développement et d'assistance	3,00
2.7		Gestion de la continuité	
	2.7.1	Prise en compte des exigences de disponibilité de l'établissement	1,00
	2.7.2	Mise en œuvre d'un plan de continuité	0,00
	2.7.3	Maintien en condition opérationnel du plan de continuité de l'établissement	0,00
2.8		Respect de la réglementation interne et externe	
	2.8.1	Respect de la réglementation externe	1,88
	2.8.2	Conformité à la réglementation interne	0,00

V. Autoévaluation : état des lieux, résultats graphiques (logiciel du GMSIH)



VI. Autoévaluation : exposition aux risques, résultats graphiques (logiciel du GMSIH)