MASTER EN SCIENCES INFORMATIQUES

Sécurisation du dossier patient informatisé en milieu hospitalier: analyse des risques et plan d'action selon la méthode EBIOS

Lahaise, Yves

Award date:
2011

Awarding institution:
Universite de Namur

Facultés Universitaires Notre-Dame de la Paix, Namur
Faculté d'Informatique
Année académique 2010-2011

Sécurisation du dossier patient informatisé en milieu hospitalier : analyse des risques et plan d'action selon la méthode EBIOS

Yves Lahaise

Mémoire présenté en vue de l'obtention du grade de master en Sciences Informatiques

Résumé

Mots clés : Dossier patient informatisé, mesures de sécurité, analyse de risques, EBIOS.

Vous travaillez dans une institution hospitalière et vous vous préoccupez de la sécurité du dossier informatisé du patient.

Une description de la composition et du contenu du dossier patient et un recensement des aspects légaux qui régissent des données à caractère personnel permettront d'aborder les besoins de sécurisation. La mise en évidence des risques encourus par le dossier patient orientera vers la nécessité de sécuriser l'accès, l'utilisation, l'intégrité et la conservation des données.

Afin de réaliser ce processus, nous avons choisi d'étudier puis d'appliquer la méthode EBIOS. Elle consiste en la définition du contexte et des objectifs de sécurité, la mise en évidence des événements redoutés, l'analyse des menaces, l'évaluation des degrés de vraisemblance et de gravité des risques, pour aboutir à l'énumération et à la planification des mesures correctrices.

Quelques conseils utiles à l'application de cette étude générale, dans une institution déterminée, seront ensuite donnés au lecteur afin qu'il puisse élaborer un plan d'action conduisant à la sécurisation de son dossier patient.

Abstract

Keywords : computerized medical record, safety measures, risk analysis, EBIOS.

You work in a hospital institution and you are concerned about the security of the computerized patient record.

A description of the composition and content of the patient record and a survey of the legal aspects that govern personal data will enable to approach security needs. Highlighting the risks to the patient record will guide to the need for securinge access, use, integrity and data retention.

To realize this process, we chose to study and then to apply the EBIOS method. It consists in defining the context and security objectives as well as the identification of feared events, threat analysis and assessment of degrees of likelihood and severity of risks, leading to the listing and planning of corrective action.

A few helpful tips for the application of this general study, in a particular institution, will then be given to the reader in order to develop an action plan leading to the security of his patient record.

Remerciements

Ecrire des remerciements, tâche difficile s'il en est.
Toutes les personnes m'ayant aidé dans cette aventure qu'est « la reprise d'études supérieures », méritent de se retrouver dans ces quelques lignes.

Je remercie d'abord cet ami (il se reconnaîtra), sans qui ces études n'auraient même pas été envisagées.

Un merci particulier à mon promoteur Monsieur Jean-Noël Colin pour son écoute, son temps et ses conseils judicieux.

Je souhaite également remercier mes enfants et ma famille pour leur soutien, pour les moments difficiles endurés par l'accumulation de travail pris sur l'horaire familial ; et tout particulièrement, mon épouse pour ses conseils et sa patience lors de la rédaction de ce travail.

Un grand merci à toutes personnes que je n'aurais pas nommées, mais qui m'ont aidé à faire fructifier ces années de travail.

Table des matières

Liste des tableaux

Table des figures

Glossaire

Médico-technique : Se dit du personnel travaillant dans des services relatifs à la santé tels que laboratoire, radiologie, salle d'examen technique ...

Para-médical : Relatif à la santé sans toutefois relever de professions médicales

Professionnel des soins de santé : On appelle profession de la santé une profession dans laquelle une personne exerce ses compétences, son jugement ou fournit un service lié au maintien, à l'amélioration de la santé des individus ou au traitement des individus blessés, malades, souffrant d'un handicap ou d'une infirmité. Conformément à l'arrêté royal n°78, sont reprises sous ce vocable, les professions suivantes :
- médecin,
- dentiste,
- sage-femme,
- pharmacien,
- kinésithérapeute,
- infirmier,
- secouriste-ambulancier,
- praticien paramédical,
- aide-soignant.

RHM : Résumé Hospitalier Minimum, combinaison des enregistrements journaliers des activités médicales et infirmières exigée par le Ministère

Introduction

A l'heure actuelle, nous laissons de plus en plus d'informations, de traces, de « morceaux d'identité » partout où nous allons. Ces traces prennent la forme d'enregistrements informatiques, elles sont très souvent soumises à des traitements divers et variés. Ce constat concerne aussi le secteur des soins de santé.

Les systèmes de santé, dont les hôpitaux font partie, sont un des grands acteurs de l'évolution sociale en Belgique. Au fil du temps, ils ont été amenés à faire face à des défis de plus en plus nombreux et complexes, notamment :

- les innovations thérapeutiques, améliorant la durée et la qualité de vie des patients,
- les progrès technologiques au service de l'élaboration d'un diagnostic,
- le vieillissement de la population, influençant les structures de soins,
- l'évolution du mode de financement du secteur des soins de santé, elle-même influencée par l'évolution de la pyramide des âges, la crise économique, les progrès de la médecine, ...,
- l'accès à un système de sécurité sociale,
- l'introduction de nombreuses, et toujours plus pointues, technologies de l'information et de la communication dans le secteur de la santé.

Ces changements ont été à l'origine d'une croissante masse d'informations recueillies à propos des patients ; informations à trier, classer et surtout archiver en vue de constituer l'histoire médicale de chaque patient.

A l'heure actuelle, la part d'informations stockée au sein des systèmes informatiques des hôpitaux et traitée par le biais des applications informatiques prend le pas sur l'archivage sous format papier. Chacune des parties constitutives d'un dossier patient est progressivement numérisée afin d'en faciliter la gestion et la consultation.

De nombreux projets, tant nationaux qu'européens préconisent de permettre la consultation de tout ou d'une partie du dossier non seulement depuis tout poste de travail situé dans l'enceinte de l'institution mais aussi depuis des accès situés en-dehors de l'hôpital. D'autres cherchent à interconnecter les centres hospitaliers,

les médecins traitants et parfois d'autres prestataires de soins.

Dès lors, la garantie de la disponibilité constante de ces données, l'importance de les traiter de manière confidentielle, l'obligation de maintenir leur intégrité et la nécessité de sécuriser leur accès doivent toujours être assurées. A cette fin, l'Etat a édicté des lois et des normes. Ces règlementations spécifiques, relatives aux systèmes d'information, en vigueur dans les hôpitaux nécessitent de fournir aux professionnels un cadre précis d'utilisation, en visant, si possible, à anticiper les modifications des directives légales.

Cette entrée dans le monde du numérique soulève de nombreuses questions :

- Quelle est la fiabilité des technologies informatiques utilisées ?
- Comment et par qui garantir la sécurisation, l'intégrité et l'accès protégé des données ?
- Comment un patient peut-il avoir la garantie que le choix qu'il a posé dans la protection de ses données personnelles est respecté ? Peut-il changer d'avis ? Peut-il les adapter ces décisions aux différents intervenants ?
- ...

Une partie de réponse se trouve dans les techniques existantes qui permettent de sécuriser la mise à disposition d'applications informatiques.

La question qui nous occupe est de valider que ces techniques sont adaptées ou adaptables à un domaine aussi particulier que le secteur des soins de santé. Autrement dit, les moyens de sécurisation de données, aussi sensibles et confidentielles que celles relatives à la santé des patients, permettent-ils de répondre aux exigences légales et aux besoins d'une institution hospitalière ?

Afin de répondre à la question, nous développerons d'abord les éléments théoriques relatifs au dossier patient et aux aspects légaux inhérents au traitement des données à caractère personnel. Ensuite, nous aborderons la notion de risques encourus et nous chercherons les mesures à mettre en œuvre afin de les gérer.

Chapitre 1

Le dossier patient

1.1 Introduction

Dans la première moitié du siècle passé, le dossier patient était le fruit d'une collecte des données se faisant oralement, voire par écrit et comportait essentiellement des informations médicales. On parlait alors de « dossier médical », il correspondait uniquement à une collection de documents relatifs à la maladie du patient.

L'évolution du concept « Santé » a prôné de ne pas se limiter à la maladie du patient, mais d'aborder plus largement son état de santé en englobant soins, prévention, éducation, ... Les informations furent étendues à :

- des données administratives,
- des données sociales,
- des données liées à la logistique,
- des données médicales,
- des données infirmières,
- des données paramédicales,
- des données de laboratoire
- des films radiologiques,
- des protocoles d'examens médico-techniques,
- ...

C'est à partir des ces ajouts que l'on en est venu à parler de « dossier patient ». Celui-ci est composé d'un ensemble de documents (physiques et/ou informatisés) qui retracent des épisodes durant lesquels la santé d'une personne a été affectée (lettres, notes, comptes-rendus, résultats de laboratoire, films radiologique, ...).

Le dossier patient doit être soigneusement conservé afin d'assurer la continuité des soins (par exemple, le dossier patient doit pouvoir être transmis à un autre médecin que celui qui a en charge le patient) et pour pouvoir répondre aux futures

demandes d'accès des patients, voire pour apporter certaines preuves en cas de recherche de responsabilité.

Face à cette mine d'informations, le besoin s'est rapidement fait sentir de les numériser, afin d'en faciliter le classement, l'archivage et le traitement ultérieur. Le passage progressif, à la fin du XXème siècle, des dossiers papier aux dossiers numérisés et l'évolution des pratiques d'archivage a soulevé des préoccupations en termes techniques (durée de vie et fiabilité des supports numériques, sécurisation des données, ...) et d'éthique médicale (confidentialité, dossiers dont la gestion est en partie sous-traitée en d'autres lieux, dans d'autres pays, par des entreprises privées, ...).

Les aspects « sécurisation » et « partage » de cette multitude d'informations de natures diverses constitueront le fil conducteur de ce travail.

1.2 Contenu

Le contenu du dossier patient est, ainsi que nous venons de le voir, très vaste. Au sein de l'hôpital, il est constitué de plusieurs sous-dossiers :

- le dossier administratif,
- le dossier médical,
- le dossier infirmier,
- le dossier des séjours aux urgences,
- les radiologies et autres protocoles,
- les résultats de laboratoire,
- ...

Même si dans la littérature et dans les aspects légaux, l'accent est souvent mis sur la partie médicale ou infirmière du dossier patient, c'est chaque partie de celui-ci qui doit pouvoir être analysée sous un angle « protection de la vie privée ».

1.3 Définition

Il n'y a pas, à proprement parler, de définition légale de ce qu'est un dossier patient, on trouve juste des mentions de ce qu'il doit au minimum comporter. Ainsi, selon l'Arrêté royal, du 03/05/1999 [Bel99], relatif au dossier médical général, on trouve dans les deux premiers articles :

1. « On entend par « dossier médical général » au sens du présent arrêté : un ensemble fonctionnel et sélectif de données médicales, sociales et administratives pertinentes relatives à un patient, qui font l'objet d'un traitement

manuel ou informatisé. Le dossier médical général a pour but d'optimaliser la qualité des soins dispensés et d'éviter les doubles emplois en ce qui concerne les actes. »

2. « Le « dossier médical général » comprend les éléments suivants : les données socio-administratives relatives au patient, l'anamnèse et les antécédents (maladies, interventions, vaccins reçus), une liste de problèmes (allergies, médications), les rapports de médecins spécialistes et d'autres prestataires de soins ainsi que les examens de laboratoire, un volet plus spécifiquement réservé au médecin généraliste et, le cas échéant, des dossiers à rubriques spécifiques. »

Compte tenu de cet arrêté, de la Loi du 07/08/1987 [Bel87] sur les hôpitaux, de la Loi du 22/08/2002 [Bel02] relative aux droits du patient, du Code de déontologie médicale (dernière version 2009), on peut affirmer, que combiné au dossier infirmier, il doit être obligatoirement ouvert pour chaque patient et contenir notamment :

- l'identité du patient,
- les antécédents familiaux et personnels,
- l'histoire de la maladie actuelle,
- les données des consultations et hospitalisations antérieures,
- les résultats des examens cliniques, radiologiques, biologiques,
- les traitements prescrits, les protocoles opératoires et d'anesthésie,
- une copie des rapports de sortie,
- les produits sanguins administrés (numéro d'unité, de série, date et heure d'administration, réactions éventuelles, ...).

Quant au dossier infirmier, d'après la Loi du 07/08/1987 [Bel87] sur les hôpitaux, la Loi du 22/08/2002 [Bel02] relative aux droits du patient et l'Arrêté royal du 28/12/2006 [Bel06], on trouve que, combiné au dossier médical, un dossier infirmier doit être obligatoirement ouvert pour chaque patient et contenir au minimum :

- l'identité du patient,
- l'anamnèse infirmière,
- les informations médicales et paramédicales,
- les traitements médicaux, les prestations techniques et les actes confiés,
- le plan de soins,
- la programmation des soins,
- une copie des rapports infirmiers de sortie.

Ils peuvent être tenus et conservés sous forme électronique.

1.4 Le dossier patient, ses aspects légaux et éthiques

La couverture légale d'un dossier patient a fortement évolué au cours du siècle passé [Hub10] :

- Avant 1930, le patient était considéré comme un objet de soins, soumis au « despotisme médical ».
- En 1936, avec « l'arrêt Mercier », on voit apparaître la notion de contrat médical avec un sujet de soins, et une exigence éthique de tenue de dossier de soins.
- En 1967, l'Arrêté royal n°78 du 10/11 relatif à l'exercice de l'art infirmier, impose l'élaboration d'un plan de soins individualisé, contenant les objectifs, les interventions et les résultats des soins.
- En 1975, le code déontologie impose de tenir un dossier de soins et émet la conception absolue du secret médical.
- En 1978, la loi sur les hôpitaux édicte, dans ses conditions d'agrément des hôpitaux, l'obligation de tenir un dossier médical et un dossier infirmier.
- En 1987, la loi du 07/08 sur les hôpitaux coordonnée et ses arrêtés royaux d'exécution, fixe les normes auxquelles les hôpitaux et leurs services doivent répondre.
- En 1992, avec la loi sur la protection de la vie privée, on en arrive à une protection de la vie privée du patient dans les différentes gestions de son dossier. On donne un cadre fonctionnel au secret médical, avec le contrôle et la maîtrise des données par le patient.
- En 1999, l'Arrêté royal du 03/05 détermine les conditions générales minimales auxquelles le dossier médical doit répondre.
- En 2002, la loi relative aux droits du patient parle de l'obligation d'un dossier tenu à jour avec un accès direct aux données, et du droit du patient à la protection de sa vie privée.
- En 2006, l'Arrêté royal du 28/12 détermine les conditions générales minimales auxquelles le dossier infirmier doit répondre.
- Le Code Pénal et son article 458, met en exergue la notion de secret professionnel.

La tenue d'un dossier patient est non seulement encadrée de manière législative, mais aussi sur le plan éthique.

Le cadre éthique trouve ses sources dans [Hub10] :

- le Code de déontologie médicale,
- les avis du « Conseil de l'Ordre des médecins »,
- le Comité d'éthique hospitalière, propre à chaque hôpital,
- les « Règles de bonnes pratiques professionnelles ».

Comme décrit, la nature du dossier patient a fortement évolué au cours du siècle passé. Le droit de la personne à la protection de sa vie privée a lui aussi fortement changé, quelles en sont les répercussions ?

Nous pouvons remarquer que deux catégories de règles, avec un champ d'application différent, sont suivies :
- celles liées au droit à la protection des données personnelles,
- celles relatives au secret médical.

Les premières s'appliquent aux données liées à une personne identifiée ou identifiable et considèrent les données médicales comme étant particulièrement sensibles.
Les secondes, concernent le secret médical qui couvre notamment la relation médecin-patient, les notes, les commentaires du praticien. Le champ d'application du secret médical est plus vaste que celui de la législation relative à la vie privée. Le secret médical est l'engagement de discrétion que le médecin prend vis-à-vis de son patient sur tous les faits (vus, entendus, recueillis) le concernant et relevés dans le décours de leur relation thérapeutique.

La protection de cette relation thérapeutique médecin-patient permet au médecin de prendre connaissance de l'entièreté des composantes physiques et/ou psychiques caractérisant son patient.

Comme le disait le philosophe britannique Francis Bacon « Savoir, c'est pouvoir » [1].

Tout en permettant d'espérer une efficacité thérapeutique maximale, cette relation pose question sur la nature du « pouvoir » que fournit cette connaissance de l'autre.
Dans le cadre de l'exercice de la médecine, cette connaissance est soumise au secret médical afin de protèger les intérêts du patient.
Toute transmission d'informations entre les différents prestataires de soins appelés à s'occuper du patient est sous-tendue par le respect du secret médical par chacun des intervenants. Le fondement du secret médical est à la fois légal [2] et déontologique [3].

1. F. Bacon a formulé en 1597,*Nam et ipsa scientia potestas est* que l'on peut traduire par « le savoir lui-même est pouvoir »
2. Article de Loi 458 du Code Pénal de 1867
3. Chapitre V du Code de Déontologie Médicale de l'Ordre des Médecins de Belgique

1.5 Conclusion

Retenons que le dossier patient est défini par son contenu pour les parties médicale et infirmière, et qu'il comprend aussi un ensemble d'autres sous-dossiers. Ce contenu est constitué de données relatives à la santé ayant une visée thérapeutique ou non : médecine préventive, diagnostics médicaux, administration de soins ou de traitements, gestion de services de santé.
Il est soumis à deux types de règles : législatives et éthiques.

Chapitre 2

Le traitement des données en regard de la Loi Vie Privée

2.1 La loi Vie Privée

Son origine remonte à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales de 1950. Dans son article 8, elle détermine le droit à l'intimité comme un droit humain : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.* » [PVE10]

Ce droit à l'intimité a progressivement évolué vers une protection des données à caractère personnel, pour en arriver, en 1981, à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Les différentes conventions ont suivi comme principe :
- la responsabilité d'au moins une personne pour chaque traitement,
- un traitement légal et justifié, en accord avec les attentes de chaque individu concerné,
- un traitement réalisé en conformité avec ce qui avait été annoncé,
- une durée de conservation des données n'excédant pas le temps nécessaire au traitement,
- une information claire et précise des individus,
- une garantie de qualité et de minimalité des données collectées,
- une garantie de sécurité dans la conservation des données,
- une catégorisation de certaines données, dites « plus sensibles »,
- un transfert des informations vers des tiers, sous certaines conditions strictes au niveau de la sécurité.

Les conventions européennes ont été transposées en droit belge, et en 1992 la Loi Vie Privée est promulguée. Le champ d'application de cette loi du 08/12/1992

concerne les données à caractère personnel ainsi que les différents traitements que l'on peut leur appliquer : traitement complètement automatisé ou non, éventuellement par le biais d'un fichier. [Bel92, Her09]

Afin de contrôler sa propre application, la loi institue la mise sur pied de la Commission Vie Privée, chargée de veiller à l'utilisation respectueuse des données à caractère personnel.

Depuis sa promulgation en 1992, la loi a subi quelques « cures de jouvence » dues, pour une part, à l'intégration en droit belge des directives européennes chargées d'harmoniser les différentes règles des états membres (Loi du 11 décembre 1998), et, d'autre part, au souhait du législateur belge de « coller » à l'évolution technologique, en modifiant le statut, la composition et les compétences de la Commission Vie Privée (Loi du 26 février 2003).

2.1.1 Données à caractère personnel

Des données sont à caractère personnel si elles concernent une personne physique, identifiée ou identifiable. Cette identification peut être directe ou indirecte, c'est-à-dire que des éléments spécifiques contenus dans les données permettent, éventuellement par recoupement, de reconnaître la personne. [Her09]

Interprétation de ces différents termes [Her09] :

1. La notion de « données à caractère personnel » est fort large, tant dans son contenu qu'au niveau du type de données. La loi parle d'ailleurs de tout type d'informations, c'est ainsi qu'aussi bien les écrits, que les sons et les images sont concernés.
2. Les données doivent correspondre à une information concernant une personne physique. Au niveau médical, un groupe de travail [1] a identifié trois groupes d'appartenance de l'information permettant de l'étiqueter de « personnelle » :
   - le contenu : l'information concerne directement un patient (son nom, son prénom, sa date de naissance, ...),
   - la finalité : l'information est utilisée ou peut être prise en compte dans le but d'évaluer, de prendre en charge ou d'influer sur l'état de santé ou le comportement d'un patient (la prise des paramètres : température, tension artérielle, ...),
   - le résultat : l'information a, in fine, un impact sur les droits ou intérêts du patient (deux traitements médicamenteux sont proposables au patient, mais avec des coûts fort différents).

   Il suffit que l'information s'intègre dans au moins un de ces groupes, pour garantir qu'elle concerne une personne physique.

1. Le groupe de travail "Article 29" sur la protection des données

3. L'identification d'une personne, physique et non morale, est le fait de pouvoir la mettre en évidence parmi un ensemble d'autres personnes. Cette identification peut être déjà réalisée ou seulement être possible. Toujours suivant le même groupe « Article 29 », cette identification est possible par de nombreux moyens allant d'un simple numéro de téléphone stocké dans la partie administrative du dossier au croisement de plusieurs caractéristiques (âge, couleur des yeux, taille, ...).

   Une réserve doit cependant être émise en ce qui concerne les critères d'identification.
   En effet, le choix de la nature et de la quantité de ces critères doit être posé en tenant compte, entre autres, des éléments suivants :
   – le rapport coûts-bénéfices lié au processus d'identification,
   – le but recherché par ce traitement,
   – les méthodes employées,
   – les intérêts des personnes qui sont susceptibles d'être identifiées,
   – les risques socio-économiques,
   – l'évolution technologique, durant la période de conservation des données (ce qui n'est pas possible à l'heure actuelle le sera peut-être demain),

   afin d'obtenir une identification pertinente, rapide et pragmatique.

2.1.2 Traitement de ces données à caractère personnel

Les traitements, évoqués par la loi, sont toutes les opérations effectuées à l'aide de procédés automatisés, en tout ou en partie, ou sans automatisation, allant de la collecte de ces données jusqu'à leur mise en fichiers, leur archivage et, in fine, leur destruction, en passant par leur enregistrement, correction, ... [Her09]

Les traitements des données à caractère personnel se doivent de respecter les concepts généraux émis par la Communauté Européenne et que nous avons énoncés dans la section 2.1.

Par contre, le législateur a relevé que certaines données avaient un caractère plus particulier et devaient être classées comme sensibles. Ce sont les informations raciales, politiques, religieuses, syndicales, sexuelles et médicales.

En particulier, pour ces dernières, la loi [2] dans son article 7 leur accorde un statut particulier : leur traitement est interdit, sauf
– si le patient a donné son accord écrit,
– s'il est nécessaire à la défense des intérêts vitaux de la personne,
– s'il correspond à une obligation légale dans le chef de la personne responsable des données,

2. Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel du 08/12/1992

– s'il est nécessaire dans un cadre thérapeutique.

2.1.3 Notion de fichier

La notion de fichier, évoquée par l'esprit de cette loi, est bien celle que l'on connaît en informatique, où le fichier est un ensemble structuré de données, ordonné selon certains critères, et auquel on peut accéder via différentes voies. Ce fichier peut être conservé de différentes manières : centralisé, décentralisé, réparti de manière fonctionnelle, ...

2.1.4 Conclusion

Au yeux de la loi sur la Vie Privée, le dossier du patient constitue bien un traitement de données à caractère personnel, automatisé ou non. Le patient y étant, par nécessité, identifié ou identifiable. Il constitue un traitement de données légitime et licite.

2.2 Les acteurs du traitement des données

D'une manière générique, on peut catégoriser les différents acteurs impliqués dans les traitements des données à caractère personnel. [PVE10] :

1. « Data Controller » et « Data Processor ». Les premiers déterminent les buts et la signification des traitements qui seront opérés sur les données, les seconds les exécutent sous la responsabilité des premiers. Cette distinction est importante dans la détermination des responsabilités vis-à-vis de la loi et des personnes concernées par les données traitées.
2. « Data Subject ». C'est la personne qui est identifiée ou qui est identifiable au travers des données en cours de traitement.

Appliqué au milieu hospitalier et pour mener à bien notre étude, il est essentiel de pouvoir identifier correctement les différentes personnes qui ont à intervenir dans le traitement de l'entièreté ou d'une partie du dossier patient.

C'est pourquoi nous considérerons comme
– « Data Controller », le responsable légal,
– « Data Processor », le personnel de l'institution hospitalière et les personnes extérieures à l'hôpital,
– « Data Subject », le patient.

2.2.1 Le patient

C'est la personne qui fait l'objet de la collecte des données. Pour des raisons évidentes, la personne identifiée, au sujet de laquelle les informations sont rassem-

blées, doit être informée et consentante au traitement de ses données. Si son état ne le permet pas, la loi prévoit qu'un représentant légal puisse être désigné.

2.2.2 Le responsable légal

Ce sera généralement le gestionnaire de l'hôpital, même si au niveau responsabilité, c'est l'hôpital qui est engagé. Il détermine les finalités du traitement des données et est soumis à toute une série d'obligations, notamment celle de s'assurer que les données sont adéquates, pertinentes et exactes. [Her09]

En matière de traitement des données du dossier patient, le responsable légal a autorité directe sur l'ensemble du personnel de l'institution hospitalière.

2.2.3 Le personnel de l'institution hospitalière

2.2.3.1 Les professionnels de la santé

C'est l'ensemble du personnel habilité à traiter les données : médecins, infirmiers, para-médicaux, personnel médico-technique. Ce sont donc, principalement, mais pas uniquement, les utilisateurs du dossier patient. Les différentes catégories de personnel, et leur fonction, doivent être correctement désignées. La liste de ces personnes doit être tenue à la disposition de la Commission de la protection de la vie privée.

Parmi eux, il convient de distinguer les professionnels des soins de santé sous la surveillance et/ou la responsabilité desquels les données sont traitées. La responsabilité semble être de nature organisationnelle, la surveillance étant le plus souvent assurée par le médecin en charge du patient et la responsabilité par le médecin-chef.

2.2.3.2 Les autres métiers

Le conseiller en sécurité de l'hôpital, qui est notamment chargé de la sécurité de l'information et qui doit conseiller les autres intervenants, en commençant par le responsable du traitement.

Le personnel administratif au sens large qui peut être amené à traiter des données (secrétaires, service informatique, ...)

2.2.4 Les personnes extérieures à l'hôpital

D'une part, l'institution hospitalière, comme toute autre entreprise, ne peut tout faire seule. Elle peut être amenée à externaliser certaines tâches (laboratoire externe, service d'imagerie médicale, sociétés de développement et de maintenance des systèmes d'informations, ...). Elle a donc recours à des sous-traitants qui

sont considérés comme des personnes physiques ou morales chargées de traiter les données pour le compte du responsable du traitement des données.

D'autre part, l'institution hospitalière est soumise à des obligations légales de faire parvenir des données à des organisations étatiques (RHM, déclaration d'épidémie, ...). Elle travaille donc pour des destinataires pour le compte desquels le traitement des données est opéré.

Par ailleurs, l'institution hospitalière peut être amenée à faire parvenir des données personnelles issues du système d'information de l'hôpital à des tiers (toute personne physique ou morale, association, administration publique, autres que celles déjà citées) qui vont traiter les données pour leur propre compte (étude pharmaceutique).

2.2.5 Conclusion

Etant donné que le dossier patient ne se résume pas seulement à un dossier médical, les acteurs opérant des traitements sur les données sont nombreux, de fonctions très différentes et pas nécessairement internes à l'institution.

2.3 Les obligations vis-à-vis du patient

Ouvrir et tenir à jour un dossier patient entraînent, pour l'hôpital, des obligations :

- disposer d'un règlement relatif à la protection de la vie privée, dont les dispositions doivent être communiquées aux patients sur support papier ou électronique,
- fournir au patient des informations minimales, sur l'utilisation des données collectées, au plus tard au moment où les données personnelles sont obtenues, qu'elles émanent directement du patient ou d'un tiers,
- déclarer auprès de la Commission de la protection de la vie privée [3] les modalités selon lesquelles il va traiter les données.

Citons également quelques droits, reconnus par la loi sur la protection de la vie privée, accordés à la personne concernée, et qui vont avoir une influence sur la manière de sécuriser les données [Her09] :

- Un droit d'information sur les traitements effectués sur ses données à caractère personnel, permettant ainsi au patient de s'opposer à tout moment à la communication de ses données d'un professionnel des soins de santé à un autre. Cette information doit être donnée au patient, en général, au plus

3. http ://www.privacycommission.be

tard au moment de la collecte. [4] On doit également tenir le patient informé de la possibilité d'introduire, le cas échéant, un recours.
- Un droit d'accès lui permettant de savoir si ses données sont traitées, comment elles le sont et avec quelles finalités. Le patient a accès au registre de la Commission de la protection de la vie privée à laquelle le responsable du traitement a fait la déclaration prescrite dans la loi sur la protection de la vie privée. Il doit pouvoir prendre connaissance, éventuellement de manière accompagnée, des informations le concernant (par exemple, pour prendre connaissance de son dossier médical).
- Un droit de rectification des données que la personne estime erronées.
- Un droit d'opposition, pour des raisons sérieuses et légitimes, au traitement de ses données.
- Un droit de suppression des données, qui en fonction de la finalité du traitement, sont incomplètes ou non pertinentes. Ce droit s'applique également aux données dépassant la limite de conservation qui leur est appliquée.
- Un droit de retirer, à tout moment, son consentement.

2.4 La conservation des données

Ces données à caractère personnel doivent être conservées de telle manière que l'identification de la personne soit toujours possible, peu importe la durée nécessaire pour atteindre la finalité des traitements qui leur est destinée.

2.4.1 Règles de conservation du dossier médical

Texte	Loi sur les hôpitaux	Code de déontologie	Loi Vie Privée	Loi droit du patient
Durée	30 ans	30 ans	Durée nécessaire à la réalisation du traitement	Pas définie

TABLE 2.1 – **Temps de conservation du dossier médical**

Dans le tableau (Cfr. table 2.1), on constate qu'en fonction de la législation servant de référence, les durées de conservation du dossier médical sont définies, laissées à l'appréciation ou indéfinies.

2.4.2 Règles de conservation du dossier infirmier

Dans le tableau (Cfr. table 2.2 page suivante) relatif aux durées de conservation du dossier infirmier, on peut voir qu'en fonction de la législation sur laquelle on se

4. C'est le rôle du règlement relatif à la protection de la vie privée

Texte	Loi sur les hôpitaux	Code de déontologie	Loi vie privée	Loi droit du patient
Durée	20 ans	Inexistant	Durée nécessaire à la réalisation du traitement	Pas définie

TABLE 2.2 – **Temps de conservation du dossier infirmier**

base, les durées sont définies, laissées à l'appréciation ou indéfinies. En Belgique, il n'y a pas encore de code déontologique spécifique à la profession infirmière.

2.4.3 Règles de conservation des dossiers médico-techniques

Si les données sont conservées en-dehors du dossier médical, des délais plus courts sont fixés par les arrêtés d'exécution de la loi du 14/07/1994 relative à l'Assurance Maladie et Invalidité :

- 2 ans pour les protocoles de radiographie,
- 2 ans pour les protocoles d'analyses de biologie clinique,
- 3 ans pour les prescriptions d'analyses de biologie clinique.

2.4.4 Destruction des données

La loi ne prévoit pas de manière explicite une procédure de destruction des données. Au contraire, elle ouvre la possibilité de les conserver au-delà des limites imposées, à des fins d'historicité, de statistiques ou scientifiques. Cette prolongation de la conservation doit se faire sous une forme, ne permettant plus l'identification de la personne concernée.

2.4.5 Conclusion

En parcourant la législation, on se rend compte d'une certaine disparité dans les règles de conservation des différents éléments du dossier patient. Dans ses choix technologiques, l'hôpital devra tenir compte de ces variations, qui pourront avoir un impact non négligeable sur les coûts engendrés.

2.5 Confidentialité des données

Il est indispensable de définir correctement le périmètre des accès au dossier patient, en fonction des responsabilités que les professionnels des soins de santé exercent dans la prise en charge de ce patient.
Garantir au patient la possibilité d'engager des poursuites en cas de non-respect des clauses de confidentialité dont il aura pris connaissance ne sera possible qu'en ayant mis en place une traçabilité complète et un moyen de conservation de ces traces d'accès aux données.

L'élaboration et l'application de ces deux procédures doit faire l'objet :
- d'une étude rigoureuse des différents profils de fonctions. Cela permettra de définir des polices d'accès précises (mot de passe, login, lien thérapeutique, ...) de qui fait quoi, quand, où, comment, ...
- d'une intégration des normes en matière de sécurité informatique, normes qui peuvent être imposées par la loi, telles que :
  - l'identification et la gestion des utilisateurs,
  - la gestion des droits accordés aux utilisateurs (lecture, création, modification, suppression),
  - la mise en place de moyens physiques de protection (antivirus, firewalls, sauvegarde, protection des réseaux, ...) ainsi que de leurs procédures d'utilisation,
  - l'instauration de moyens de surveillance des actions ou des opérations effectuées,
  - l'application, si nécessaire, de moyens d'anonymisation des données,
  - ...

2.6 Droit de plainte

La loi prévoit qu'à tout moment, la personne concernée par les données à caractère personnel peut se prévaloir d'un recours envers la personne responsable du traitement de celles-ci, pour autant qu'elle puisse prouver un acte contraire aux règles édictées.

2.7 Conclusion

En regard des évolutions technologiques et sociales, la loi devrait idéalement être actualisée aussi rapidement que possible, voire même prendre les devants. Ces adaptations, si fréquentes soient-elles, devraient être suivies par un « comité de vigilance » et appliquées au niveau organisationnel par un renforcement des politiques mises en œuvre pour protéger les données.

Notons toutefois, que dans le cadre du dossier patient, il y a un risque d'antagonisme entre les droits du patient et l'obligation, pour les professionnels en soins de santé, de tenir un dossier conforme aux prescrits légaux et à leur obligation de veiller à la qualité des soins et à la sécurité du patient ou des tiers.

Une application stricte de la loi devrait permettre de garantir toute la sécurité des données du dossier patient.
Cependant elle ne se suffira pas à elle-même si on ne met pas en place toute une série de mesures destinées à contrecarrer ou à diminuer la gravité des risques

encourus inhérents à différentes menaces sur l'environnement, sur les personnes et pouvant avoir des origines humaines ou environnementales, internes ou externes, accidentelles ou intentionnelles. Ce point sera abordé au chapitre suivant.

Chapitre 3

Des risques pour le dossier patient informatisé ?

Comme nous venons de le voir, la gestion des données personnelles au sein d'un hôpital est soumise à un ensemble de règles légales et éthiques.

Si le législateur et les différents organes « éthiques » ont jugé bon de les établir, c'est que ces informations, gérées au sein d'un dossier patient informatisé, courent un certain nombre de risques. [GVT01]

Selon le CLUSIR Rha[1] les risques peuvent être classés selon deux axes (Cfr. figure 3.1 page suivante).
Le premier est l'axe variant du Physique à l'Humain. En le suivant, on trouve, d'un côté, des risques touchant ou émanant du matériel et à l'autre extrême, des risques impliquant les personnes.
Le deuxième axe est celui qui relie le Fortuit à l'Intentionnel, il permet le classement des risques en prenant en compte le caractère intentionnel de l'auteur.

Cette typologie des risques peut-elle s'appliquer aux risques courus par les données personnelles du dossier patient au sein d'un hôpital ?

Pour pouvoir répondre à cette question, nous allons classer les données du dossier patient selon plusieurs critères :

- leur fonction : administratives, médicales, statistiques, ...,
- leur type : textes, images, sons, ...,
- leur stabilité dans le temps : fortement ou peu modifiées,
- leur degré et rythme de consultation : consultations fréquentes, occasionnelles, rares mais importantes quand elles le sont,
- leur durée de conservation : court, moyen ou long terme,
- leur durée de mise à disposition : limitée, permanente.

1. Club de la Sécurité du Système d'information Rhônes-Alpes

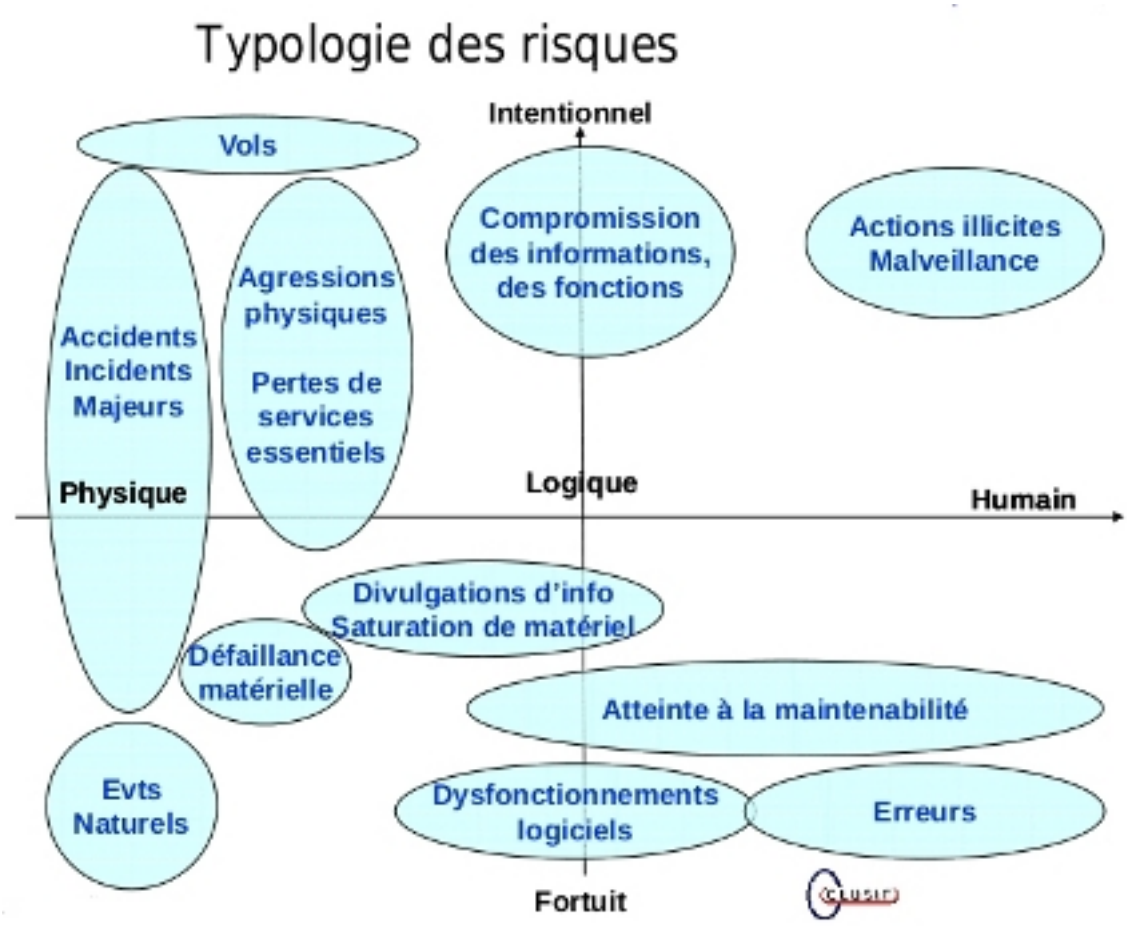


FIGURE 3.1 – **Typologie des risques**

Il est évident que des recouvrements existent entre les différents critères. Ainsi une information administrative, par exemple le nom d'un patient, n'est généralement pas modifiée, mais est continuellement utilisée au sein du dossier patient et sera conservée durant tout le prescrit légal.

Le classement d'une donnée en fonction des différents critères évoqués permet d'aborder la typologie du CLUSIR avec plus de précision.
En effet, une donnée « brute » du dossier patient peut être caractérisée par les différents critères et la donnée ainsi détaillée sera plus facilement introduite dans la typologie du CLUSIR.
En se focalisant sur un critère particulier, on peut limiter les risques rencontrés et ainsi mettre en évidence des mesures de sécurité plus faciles à instaurer.

Reprenons cette donnée, le nom du patient, et identifions les risques qu'elle

encoure selon la typologie du CLUSIR :

- Evénements naturels : inondation ⇒ perte de la donnée.
- Accidents, incidents majeurs : incendie ⇒ perte de la donnée.
- Vols : vol de la machine hébergeant la base de données ⇒ perte de la donnée si « simple vol », ⇒ divulgation de la donnée si vol avec exploitation des informations contenues sur le support.
- Défaillances matérielles : crash disque ⇒ perte de la donnée.
- Dysfonctionnements logiciels : une modification de la donnée est permise ⇒ donnée corrompue.
- Divulgations d'informations : divulgation fortuite d'informations lors de discussions de « couloir » ⇒ donnée compromise.
- Erreurs : encodage sur un mauvais patient ⇒ donnée corrompue.
- Atteintes à la maintenabilité : changement d'applications ⇒ donnée corrompue.
- Actions illicites, malveillances : divulgation intentionnelle d'information ⇒ donnée compromise.
- Compromissions des informations, des fonctions : accès à l'information par un personnel non autorisé ⇒ donnée compromise.

A partir de ce simple exemple, on se rend compte qu'une donnée basique est soumise à un ensemble de menaces et que, par extrapolation, c'est tout le système d'information qui doit être concerné par une étude des risques. Il devra être sécurisé afin de répondre aux exigences légales et éthiques.
Pour envisager la sécurité d'un système d'information, nous allons nous pencher sur les différentes menaces qui pèsent sur lui et qui risquent d'altérer les données qu'il maintient.

Différentes méthodes d'analyse de ces menaces existent, citons par exemple :

- la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité),
- la méthode MEHARI (MEthode Harmonisée d'Analyse des Risques),
- la méthode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation),
- la métode NAIMS (National aerospace Infrastructure Management System),
- la méthode FEROS (Fiche d'Expression Rationnelle des Objectifs de Sécurité).

Elles cherchent à évaluer la sécurité sous différents angles, permettant de distinguer différentes atteintes visant les trois grands domaines de la sécurité que sont

- l'intégrité : c'est la caractéristique qui certifie qu'une donnée représente bien ce qu'elle doit représenter,
- la confidentialité : c'est la caractéristique qui fait qu'une information n'est

accessible qu'à l'entité (personne, système) qui y est autorisée,
– la disponibilité : c'est la caractéristique qui spécifie que les données doivent être accessibles pendant des périodes de temps précises.

Ces atteintes aux données peuvent être le fait de toute une série de menaces liées aux personnes, aux programmes, aux événements extérieurs.
Face à ces menaces, les différentes méthodes mettent en évidence la gravité des risques que courent les informations, ainsi que la probabilité d'occurrence des menaces. Chacune d'elles les classent et les scorent afin de pouvoir les comparer.

Les objectifs de sécurité ayant été déterminés, les risques et les menaces classés, il reste à définir les politiques de sécurité à suivre pour pallier ou corriger les risques encourus. On gardera, en toute conscience, une série de risques dits résiduels dont l'apparition est peu probable ou dont les conséquences seraient peu ou pas préjudiciables pour l'institution.

Les objectifs de sécurité se rapportent aux trois domaines cités dans le paragraphe précédent, auxquels, suivant le Référentiel Général de Sécurité [ANS10c], nous pouvons ajouter :
– la confidentialité des éléments critiques du système d'information : principe identique à la confidentialité des données, vue précédemment, mais touchant spécifiquement le « matériel » du système d'information,
– l'authentification : processus qui permet à une personne, à un système, de se faire reconnaître d'une autre personne, d'un autre système au moyen d'éléments définis,
– la traçabilité : c'est la conservation et l'exploitation des traces de l'ensemble des actions effectuées. Par « traces » on entend l'auteur, la nature, le déroulement de l'action.

Nous allons utiliser la méthode EBIOS 2010 [ANS10b] qui se veut une boîte à outils modulaire, évolutive et alignée avec les normes [2] [3] [4] pour permettre tout type de réflexion sur la sécurité des systèmes d'information.

Le champ d'investigation de la méthode est suffisamment générique que pour permettre son utilisation dans des domaines très variés (sécurité de l'information, sécurité des infrastructures, ...) et à des degrés plus ou moins approfondis.
On peut commencer par étudier le domaine concerné de manière globale puis se focaliser sur des sous-systèmes.

2. ISO 27001 : Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences
3. ISO 27002 : Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information
4. ISO 27005 : Technologies de l'information - Techniques de sécurité - Gestion du risque en sécurité de l'information

L'étude réalisée peut toujours être reproduite et ainsi vérifiée, validée et généralisée. Elle peut donc être considérée comme fiable.

Elle offre également, par ses résultats, une bonne base de sensibilisation, de négociation et d'arbitrage face aux différents acteurs de la chaîne de décision.

Chapitre 4

La méthode EBIOS appliquée au dossier patient informatisé

4.1 Description

FIGURE 4.1 – **Description de la démarche EBIOS**

La méthode EBIOS est une étude itérative comportant 5 modules au cours desquels on sera amené à se poser une série de questions, comme on peut le voir sur la figure 4.1 [ANS10a].

Chaque module aura son rôle dans la démarche continue d'évaluation :

Module 1. Etude du contexte : il permet de définir le périmètre étudié, les métriques utilisées pour la collecte des informations nécessaires ainsi

que les paramètres et contraintes à considérer.

Module 2. Etude des événements redoutés : il permet l'expression de ceux-ci à partir de l'identification et de l'estimation des besoins de sécurité, des sources de menaces à l'origine du non-respect des besoins et des impacts en résultant. Le module est axé sur les biens essentiels.

Module 3. Etude des scénarii de menaces : il permet, à partir de l'identification, de l'estimation et de la combinaison des scénarii de menaces provoquant les événements redoutés du second module, de composer les risques. Il est axé sur les vulnérabilités des biens supports.

Module 4. Etude des risques : il combine les résultats des deux modules précédents pour identifier les risques encourus par les besoins de sécurité à atteindre en fonction du périmètre défini au premier module. Il regroupe les risques selon la nécessité de leur traitement.

Module 5. Etude des mesures de sécurité : il envisage le traitement des risques à l'aide de ces dernières à partir de leur spécification, planification et validation. Il confirme le caractère résiduel de certains risques.

Chaque module se décompose en une ou des activités, elles-mêmes constituées d'une ou de plusieurs actions. Chaque module étudié respectera cette structure.

4.2 Module 1 : Etude du contexte

4.2.1 Définir le cadre de la gestion des risques

« *Cette activité fait partie de l'établissement du contexte. Elle a pour but de circonscrire le périmètre d'étude et de définir le cadre dans lequel la gestion des risques va être réalisée.* » [ANS10b]

4.2.1.1 Cadre de l'étude

L'objectif de l'étude est de veiller au respect des prescrits légaux et éthiques qui régissent l'utilisation de données personnelles dans un dossier patient au sein d'un hôpital.

Pour cela, nous devons étudier les risques encourus par le traitement de ces données. Cette étude se fera de manière théorique, nous n'étudierons pas le cas d'un hôpital particulier. Nous essayerons plutôt d'apporter des pistes de solutions aux personnes concernées par la prise de décision en matière de sécurité des données au sein d'un tel établissement, personnes qui auront été identifiées au préalable.

4.2.1.2 Contexte général

Dans le cadre de la définition de notre contexte général, outre le dossier patient tel que présenté au chapitre 1, il faut tenir compte d'un ensemble de facteurs qui renforcent encore la spécificité d'un hôpital par rapport à une société, dite, commerciale [GVT01] :

- la diversité des activités médicales, chirurgicales et médico-techniques, avec leurs risques particuliers,
- le large spectre des catégories professionnelles que l'on y rencontre,
- la complexité des lignes hiérarchiques (médicale, infirmière, administrative, ...),
- la structure d'un hôpital et sa constante mutation architecturale, confiée bien souvent à des acteurs externes, augmentant ainsi les allées et venues naturelles au sein du bâtiment,
- la participation au plan MASH (Mise en Alerte des Services Hospitaliers) ou autre plan d'urgence exceptionnel faisant intervenir des organismes officiels.

Un hôpital est un lieu de soins et/ou d'examens, où dans le cadre de la prise en charge du patient, le système de gestion des données ne doit donner l'accès qu'aux informations nécessaires et pas plus. Plus qu'ailleurs le personnel est amené à une grande mobilité, facteur dont nous allons devoir tenir compte.
Par « personnel », il faut comprendre le personnel lié à l'hôpital par un contrat de travail, mais aussi toutes les personnes en cours de formation (médecin, infirmier, para-médicaux, informaticien, électricien, ...). Ces « étudiants » doivent pouvoir accéder aux données nécessaires à leur activité. Cette catégorie a un turn-over encore plus important que l'autre, ce qui intensifie les allées et venues du personnel dans le système d'information.

L'augmentation exponentielle de la quantité et des types de données à sauvegarder ou à maintenir pour des périodes plus ou moins longues, dans le respect de la loi, provoque également une augmentation de l'exposition aux risques dans les services concernés.

L'hôpital est également un lieu privilégié pour collecter des données en vue d'études diverses (pharmaceutiques, médicales, ...). On y rencontre donc un besoin d'anonymisation ou de pseudo-anonymisation des données afin de garantir la protection de la vie privée des personnes concernées. Rappelons que certaines caractéristiques d'une personne permettent déjà de l'identifier si le groupe dont elle fait partie est petit.
Citons encore l'émergence de nombreux projets tels que ECare, eHealth, ... [VB03]. Tout intéressant que soient leurs contenus et leurs implications, ils ne feront pas partie des suites de ce travail.

De plus en plus d'équipements, médicaux ou autres, dépendent d'une connexion sur le réseau de l'hôpital ou sur le « Web » pour fonctionner. Cette dépendance entraîne également une série de risques, le réseau devenant une pierre angulaire et vitale de l'infrastructure hospitalière. Sont concernés ici les multiples moyens mobiles (portable, Ipad, smartphone, ...) permettant d'accéder aux données stockées dans le système d'information d'un hôpital, ils entraînent une augmentation conséquente des risques encourus par les données.

L'émergence de nouvelles technologies amène, avec elles, l'apparition de nouveaux risques. Par exemple, la numérisation des examens radiologiques mis à disposition sur le « Web » pour permettre à un médecin situé à l'extérieur de l'hôpital de protocoler l'examen, entraîne une dépendance accrue par rapport à la connexion existante, ce qui la rend d'autant plus sensible à une surcharge du trafic par un pirate.

Dans ce contexte général la demande est grande d'une gestion efficace des informations relatives à des populations de plus en plus impliquées dans leur prise en charge thérapeutique. Il faut pouvoir identifier les personnes soignées, sans risque d'erreur, et cela en dépit des contraintes temporelles ou de localisation de l'information afin de leur garantir une prise en charge efficace.

Dans cette gestion des risques, les rôles et les responsabilités sont partagés entre les différentes personnes reprises dans la section 2.2 page 12.

4.2.1.3 Périmètre de l'étude

Nous limiterons volontairement le périmètre de l'étude à l'analyse des risques, menaces et objectifs de sécurité à l'égard des données personnelles contenues dans le dossier patient en rapport avec le cadre légal et éthique décrit au chapitre 2. Nous concentrerons notre analyse sur le dossier patient, interne à un hôpital, sans tenir compte des mutualisations de dossiers inter-hospitaliers en cours de développement.

De la même manière, les réseaux informatiques des hôpitaux pouvant être de natures fort diverses, nous citerons quelques grands principes et généralités, qui seront à garder à l'esprit lors de leur construction.

Les enjeux identifiés sont donc :
- favoriser la prise en charge thérapeutique pour un ensemble hétérogène de personnes, la réussite de l'implémentation d'un dossier patient étant intimement liée à la confiance que peuvent lui faire les utilisateurs,
- garantir, dans la gestion des données personnelles, un respect des droits du patient selon le cadre légal,

– garantir la confidentialité et le respect des finalités dans le traitement des données personnelles du dossier patient,
– garantir la sécurité d'un dossier patient, c'est pour l'institution se prémunir contre des attaques en justice.

4.2.1.4 Paramètres à prendre en compte

Les données du dossier patient sont de nature tellement sensible que nous exprimerons ces paramètres sous forme de contraintes :

– Contraintes légales : détaillées aux deux premiers chapitres.
– Contraintes budgétaires et conjoncturelles : ce sont des contraintes induites par le mode de financement appliqué aux hôpitaux et associées à une recherche constante d'optimisation des coûts.
– Contraintes sociales : les hôpitaux sont situés dans des bassins de soins extrêmement variés sur le plan des conditions sociales dans lesquelles vit leur population.
– Contraintes temporelles sur les délais de développement et d'implémentation des logiciels : le temps qui s'écoule entre les prises de décision et leur mise en œuvre est parfois long.
– Contraintes de personnel déjà évoquées, auxquelles il faut ajouter l'obligation d'utiliser l'informatique sans en avoir au préalable les notions de base.
– Contraintes de disponibilité : 24h/24h et 7 jours sur 7, avec un temps moyen d'inactivité limité au maximum. Il est obligatoire de prévoir des plans de continuité et des plans de reprise après incident.
– Contraintes de qualité et de fiabilité des données : les données ne doivent pas être corrompues.
– Contraintes géographiques : suite à des fusions ou regroupements, les hôpitaux sont établis sur plusieurs sites et doivent donc adapter la gestion des données en conséquence (différence de format, transfert d'information, ...).
– Contraintes médiatiques : pression du public et des médias qui attendent beaucoup du monde médical et qui n'hésitent pas à pointer du doigt les moindres défaillances.

4.2.1.5 Sources des menaces

Les menaces qui pèsent sur les données personnelles peuvent être le fait de personnes internes ou externes à l'institution, agissant de manière accidentelle ou intentionnelle, avec des capacités plus ou moins développées. Elles peuvent aussi être le fait de sources non humaines.

Dans le tableau qui suit (Cfr table 4.1 page 32), chaque menace sera décrite par sa source, le domaine qu'elle atteint et la nécessité de la traiter, elle sera illustrée par des exemples.

Sources des menaces	Domaines	A traiter	Exemples
Source humaine interne, malveillante, avec de faibles capacités	– Confidentialité – Intégrité	Oui	– Technicien de surface utilisant un pc non verrouillé – Personnel écoutant les conversations entre les autres membres du personnel soignant
Source humaine interne, malveillante, avec des capacités importantes	– Disponibilité – Confidentialité – Intégrité	Oui	– Utilisateur outrepassant ses droits d'accès, pour une utilisation abusive des données – Utilisateur usurpant l'identité d'un autre utilisateur – Utilisateur effaçant des données patient – Gestionnaire ou utilisateur effaçant des traces de ses actions
Source humaine interne, malveillante, avec des capacités illimitées	– Confidentialité	Oui	– Personnel ayant des accès illimités aux données et détournant les finalités du traitement
Source humaine externe, malveillante, avec de faibles capacités	– Disponibilité	Oui	– Personne volant du matériel, dans un simple but de revente de pièces

Suite page suivante

Sources des menaces	Domaines	A traiter	Exemples
Source humaine externe, malveillante, avec des capacités importantes	– Confidentialité	Oui	– Membre d'une firme extérieure usurpant l'identité d'un membre du personnel – Personne d'une société de maintenance écoutant les conversations ou récupérant des documents papiers
Source humaine externe, malveillante, avec des capacités illimitées	– Disponibilité – Confidentialité – Intégrité	Oui	– Personne écoutant le réseau wifi pour voler des données ou dans un but de sabotage – Personne s'attaquant aux données stockées de manière externe à l'institution
Source humaine interne, sans intention de nuire, avec de faibles capacités	– Disponibilité	Oui	– Membre du personnel débranchant de manière intempestive des machines – Patient entravant de manière délibérée la diffusion des informations le concernant
Source humaine interne, sans intention de nuire avec des capacités importantes	– Intégrité	Oui	– Personnel méconnaissant les procédures de sauvegarde/restauration – Personnel mal formé

Suite page suivante

Sources des menaces	Domaines	A traiter	Exemples
Source humaine interne, sans intention de nuire, avec des capacités illimitées	– Confidentialité – Intégrité	Oui	– Personnel de maintenance informatique diffusant le l'information lors de discussions hors institution
Source humaine externe, sans intention de nuire, avec de faibles capacités	– Confidentialité	Oui	– Patient curieux – Visiteur curieux
Source humaine externe, sans intention de nuire, avec des capacités importantes	– Confidentialité	Oui	– Professionnel utilisant des données exportées à des fins statistiques
Source humaine externe, sans intention de nuire, avec des capacités illimitées	– Confidentialité	Oui	– Firme extérieure gérant les bases de données
Virus non ciblé	– Disponibilité – Confidentialité – Intégrité	Oui	
Catastrophe naturelle ou sanitaire	– Disponibilité – Intégrité	Oui	– Phénomène naturel (foudre, usure...)
Activité animale	– Intégrité	Non	– Rongeur dans la salle machine
Événement interne	– Disponibilité – Intégrité	Oui	– Panne électrique – Problèmes sur le réseau – Incendie des locaux

TABLE 4.1 – **Sources des menaces**

4.2.2 Préparer les métriques

« *Cette activité fait partie de l'établissement du contexte. Elle a pour but de fixer l'ensemble des paramètres et des échelles qui serviront à gérer les risques. Elle peut être commune à plusieurs études.* » [ANS10b]

4.2.2.1 Critères de sécurité et échelles des besoins

Comme besoins de sécurité pour le dossier patient, nous retiendrons les différents domaines cités page 21 :

1. **La disponibilité** : le dossier patient devrait idéalement être accessible tous les jours et à toute heure afin de correspondre aux attentes des utilisateurs. En fonction des possibilités technologiques offertes, la disponibilité devra surtout être guidée par leur seuil de tolérance (chacun estime la notion d'indisponibilité de manière différente et subjective).
   Le besoin en disponibilité tient à la fois compte d'une interruption maximale et d'une durée cumulée d'indisponibilité (Cfr table 4.2).

Niveau	Description du niveau de disponibilité
4	Hautement disponible : le temps cumulé d'indisponibilité des données est < à 10H par an et composé de périodes de moins de 1H
3	Très disponible : le temps cumulé d'indisponibilité des données est < à 20H par an et composé de périodes de moins de 2H
2	Disponible : le temps cumulé d'indisponibilité des données est < à 40H par an et composé de périodes de moins de 4H
1	Peu disponible : le temps cumulé d'indisponibilité des données est > à 40H par an et composé de périodes de plus de 4H

TABLE 4.2 – **Echelle du besoin en disponibilité**

2. **L'intégrité** : le dossier patient doit être le strict reflet du patient concerné. Les professionnels l'utilisant ont besoin que les données qu'il contient soient complètes, exactes, inaltérables et/ou récupérables (Cfr table 4.3).

Niveau	Description du niveau d'intégrité
4	Les données sont conservées : totalement intègres et protégées
3	Les données sont récupérables : elles ont été corrompues mais leur intégrité est récupérable
2	Les données sont perdues : elles ont été corrompues et leur intégrité n'est pas récupérable
1	L'état d'intégrité des données est inconnu

TABLE 4.3 – **Echelle du besoin d'intégrité**

3. **La confidentialité des données** : les données contenues dans le dossier patient ne doivent être échangées et utilisées que par les personnes dont l'activité le requiert. Celles-ci ont besoin que le caractère plus ou moins confidentiel et/ou privé des données qu'elles encodent dans le dossier patient respecte certains niveaux (Cfr table 4.4). Elles doivent éventuellement pouvoir introduire dans le dossier patient des données qui restent à leur seule disposition.

Niveau	Description du niveau de confidentialité des données
4	Les données sont confidentielles : strictement réservées à la personne qui les a encodées
3	Les données sont privées : partageables entre prestataires de soins, identifiés, ayant en charge le patient ou avec les entités externes reconnues
2	Les données sont réservées : partageables au sein de l'hôpital, par des personnes identifiées ou avec les entités externes reconnues
1	Les données sont publiques : strictement anonymisées et partageables avec l'extérieur de l'hôpital

TABLE 4.4 – **Echelle du besoin en confidentialité des données**

4. **L'authentification** : quelle que soit le degré de confiance envers le personnel de l'institution ou son aversion au concept de sécurité, certains niveaux d'authentification sont nécessaires pour accéder aux applications, aux machines, aux locaux.
   Il faut ici rappeler la distinction entre l'identification (communiquer d'une identité) et l'authentification (apporter la preuve de l'identité que l'on avance).
   Les niveaux d'authentification seront fonction des types de données protégées (Cfr table 4.5).

Niveau	Description du niveau d'authentification
3	Une authentification personnelle est nécessaire
2	Une authentification individuelle ne doit pas être garantie, l'appartenance à un groupe, un rôle est suffisante
1	Pas d'authentification

TABLE 4.5 – **Echelle du besoin en authentification**

5. **La traçabilité** : dérivant des critères de confidentialité et d'intégrité, ce critère impose de conserver l'association auteur-action, aussi longtemps, si pas plus que les données. [San09]
   Ce critère est à la fois une obligation légale et une manière de garantir aux professionnels de la santé ainsi qu'aux personnes desquelles on conserve les données que l'on pourra toujours retrouver l'individu qui a créé/consulté/modifié/imprimé/transmis les données (Cfr table 4.6 page suivante).

Niveau	Description du niveau de traçabilité
3	Une traçabilité complète (Qui/Quoi/Où/Comment) et conservée, aussi longtemps que les données auxquelles elles se réfèrent, doit être mise en place
2	La traçabilité mise en place n'est pas complète (Qui/Quoi/Où/Comment), il manque au moins un des éléments
1	Aucune traçabilité

TABLE 4.6 – **Echelle du besoin en traçabilité**

6. **La confidentialité des éléments critiques du système d'information** : au même titre que les données, ils doivent être sécurisés car la connaissance du mode de fonctionnement du système d'information fournit à son propriétaire un pouvoir immense sur celui-ci, lui permettant ainsi d'exploiter les failles plus facilement et plus rapidement.
   Même si le RGS [1] [ANS10c] la retient comme un besoin de sécurité, nous la traiterons, dans le module 5, à travers les mesures portant spécifiquement sur certains matériels du système d'information.

4.2.2.2 Echelle des niveaux de gravité

La sécurité des données personnelles est d'une telle importance dans le cadre du dossier patient, qu'il ne doit pas, à notre sens, y avoir de demi-mesure.
Cependant, afin de pouvoir traiter de manière précise et hiérarchisée les risques et scénarii de menaces par la suite , nous donnerons les niveaux de gravité suivants : majeure, importante, négligeable et nulle (Cfr table 4.7 page suivante).
Pour déterminer le niveau de gravité d'une menace, nous nous servirons des besoins exprimés dans les paragraphes précédents.

Chaque donnée du dossier patient sera analysée en fonction de chacune des premières échelles (Cfr tables 4.2 page 33, 4.3 page 33, 4.4 page précédente, 4.5 page précédente, 4.6). Si la menace que l'on analyse empêche le besoin d'être rencontré, alors on dira que le niveau n'est pas atteint.

Dans le contexte d'une institution précise, les différentes parties prenantes de la gestion de la sécurité des systèmes d'information fixeront les niveaux de gravité des menaces par consensus.

4.2.2.3 Echelle des niveaux de vraisemblance

Cette échelle doit permettre de déterminer avec facilité et sans ambiguïté le degré de vraisemblance qu'une menace survienne.
Ainsi une menace qui va se produire avec comme seule restriction la notion de

1. Référentiel Général de Sécurité

Niveau	Description du niveau de gravité
4	La gravité est majeure : la sécurité du dossier patient est compromise. Des données concernant un patient sont susceptibles d'être diffusées hors de l'hôpital, l'impact légal est critique pour l'institution.
3	La gravité est importante : la sécurité du dossier patient est compromise. Des données concernant un patient sont susceptibles d'être connues dans l'hôpital, par tout type de personne, l'impact légal est critique pour l'institution si les faits sont avérés.
2	La gravité est négligeable : la sécurité du dossier patient est compromise. Des données concernant un patient sont susceptibles d'être diffusées dans l'hôpital, parmi du personnel soumis au secret professionnel, mais ne prenant pas en charge ce patient, l'éthique suivie par l'institution est compromise.
1	La gravité est nulle : la sécurité du dossier patient n'est pas compromise.

TABLE 4.7 – **Echelle des niveaux de gravité**

délai qualifiera la vraisemblance de la menace de certaine. Si pour se déclencher la menace à besoin que plusieurs facteurs soit présents, alors on la qualifiera de probable. Si à cette combinaison, on ajoute le critère temps, alors la vraisemblance de la menace devient faible. Par contre si quelle que soit la combinaison de critères et quel que soit le temps qui passe, la menace ne peut se produire, on dira que sa vraisemblance est nulle (Cfr table 4.8).

Niveau	Description du niveau de vraisemblance
4	La menace va certainement se produire, dans un délai plus ou moins court
3	La menace va probablement se produire si certains facteurs sont réunis
2	La menace a peu de chance de se concrétiser car elle nécessite une combinaison de plusieurs facteurs sur un laps de temps prolongé
1	La menace ne se produira pas

TABLE 4.8 – **Echelle des niveaux de vraisemblance**

4.2.2.4 Critères de gestion des risques

L'ensemble des paramètres, des besoins en sécurité et les échelles étant élaborés, il est nécessaire de définir comment ils seront utilisés dans la suite de l'étude. L'objectif étant de définir la manière d'estimer, d'évaluer et de classer les menaces, les risques, les scénarii d'exécution, les résultats obtenus ainsi que les risques résiduels à l'aide des échelles précédentes (Cfr table 4.9 page suivante).

Suite page suivante

Gestion des risques	Description des règles choisies

Gestion des risques	Description des règles choisies
Analyse des événements redoutés (module 2)	Ils sont analysés en termes de gravité à l'aide de l'échelle 4.7 page précédente
Évaluation des événements redoutés (module 2)	Ils sont classés par ordre décroissant à l'aide de l'échelle 4.8 page précédente
Analyse des scénarii de menaces (module 3)	Ils sont analysés en termes de vraisemblance à l'aide de l'échelle 4.8 page précédente
Évaluation des scénarii de menaces (module 3)	Ils sont classés par ordre décroissant à l'aide de l'échelle 4.8 page précédente
Analyse des risques (module 4)	Un risque est la combinaison d'un événement redouté, et d'un ou plusieurs scénarii de menaces. Dès lors son analyse consiste à reprendre la gravité de l'événement et la vraisemblance maximale des scénarii de menaces qui peuvent le provoquer.
Évaluation des risques (module 4)	Les risques catégorisés en gravité et en vraisemblance seront introduits dans le tableau 4.10 page suivante afin de déterminer si leur traitement est nécessaire, facultatif ou inutile.
Choix de traitement des risques (module 4)	Le traitement des risques devra permettre de faire descendre le niveau de gravité et/ ou de vraisemblance afin de catégoriser plus légèrement le risque.
Analyse des risques résiduels (module 4 et 5)	Bien que faisant partie des risques dont le traitement est considéré comme inutile, ils seront analysés comme s'ils étaient seuls (les autres risques ayant trouvé un traitement approprié) afin de bien les mettre en évidence et d'être certain qu'ils sont connus des différentes parties prenant part aux décisions de sécurité.
Choix des mesures de sécurité (module 5)	Les différentes mesures seront choisies afin d'agir sur le niveau de gravité et/ou de vraisemblance des risques.
Homologation de sécurité (module 5)	L'homologation finale ne sera effective que lorsque les mesures de sécurité choisies, tenant compte des contraintes éventuelles, seront planifiées et que le contrôle de leurs résultats sera mis sur pied.

TABLE 4.9 – **Critères de gestion des risques**

Dans le tableau 4.10 page suivante, un risque dont les impacts seraient qualifiés de majeurs (gravité 4) et dont la vraisemblance des scénarii seraient certaine (vraisemblance 4), se situerait dans l'angle du tableau impliquant l'obligation pour l'institution de prendre les mesures nécessaires à contrecarrer, ou à corriger, l'apparition du risque.
A l'inverse, un risque qualifié par une gravité négligeable (gravité 1) et dont la vrai-

semblance des scénarii est nulle (vraisemblance 1), ne nécessiterait pas la prise de mesures de la part de l'institution.

Gravité	4	Souhaitable	Nécessaire	Nécessaire	Nécessaire
	3	Inutile	Souhaitable	Nécessaire	Nécessaire
	2	Inutile	Souhaitable	Souhaitable	Nécessaire
	1	Inutile	Inutile	Souhaitable	Souhaitable
		1	2	3	4
		Vraisemblance			

TABLE 4.10 – **Evaluation du besoin de traitement des risques**

4.2.3 Identifier les biens

« *Cette activité fait partie de l'établissement du contexte. Elle a pour but d'identifier les biens au sein du périmètre de l'étude et ainsi de mettre en évidence les éléments nécessaires aux autres activités.* » [ANS10b]

4.2.3.1 Les biens essentiels

Le bien essentiel est le contenu du dossier patient comme décrit dans l'introduction du chapitre 1 avec les subdivisions suivantes :
- le dossier administratif,
- le dossier médical,
- le dossier infirmier,
- les radiologies et autres protocoles,
- les résultats de laboratoire.

Le dossier des urgences étant souvent intégré dans la partie médicale ou dans la partie infirmière, ne sera pas analysé séparément.

Nous avons choisi cette subdivision car si chacune des parties du dossier est sous la responsabilité finale du gestionnaire de l'hôpital, leurs propriétaires et utilisateurs principaux diffèrent.
Les données gérées par chacune de ces parties sont relativement similaires dans leurs types, mais différentes par leur degré de conservation temporelle. Elles sont gérées par des systèmes qui tout en communiquant l'un avec l'autre sont distincts.

4.2.3.2 Les biens supports

Dans cette rubrique, nous recensons des biens techniques et non-techniques, communément utilisés et venant en support aux différentes parties du dossier patient.

Suivant la méthode EBIOS, les biens supports peuvent être classés en trois grandes familles et plusieurs sous-familles :

- SYS : systèmes informatiques et de téléphonie
  - MAT : matériels
  - LOG : logiciels
  - RSX : canaux informatiques et de téléphonie
- ORG : organisations
  - PER : personnes
  - PAP : support papier
  - CAN : canaux interpersonnels
- LOC : locaux

En milieu hospitalier, pour assurer le suivi du dossier patient, sont généralement utilisés :

- MAT : les différents matériels équipant les réseaux filaires,
- RSX : le réseau filaire en lui-même,
- MAT : les différents matériels équipant les réseaux wifi, de plus en plus présents dans les institutions hospitalières, et que nous traiterons séparément du point MAT,
- RSX : le wifi en lui-même,
- LOG : les différents systèmes de gestion de bases de données (Oracle, SQL-Serveur, PostgreSQL, ...),
- LOG : les différentes applications utilisées pour gérer les données,
- MAT : les différents PC et serveurs,
- LOG : les différents OS utilisés,
- MAT : les différentes solutions de stockage (SAN, ...),
- LOG : les différents logiciels embarqués au sein des appareillages utilisés en radiologie, salle d'opérations, soins intensifs, ...,
- PAP : tous les documents imprimés,
- CAN : on trouvera essentiellement ici les discussions que tout un chacun a avec ses pairs sans toujours tenir compte de l'endroit où il est à ce moment là,
- PER : l'ensemble des fonctions présentes au sein de l'hôpital,
- LOC : les salles serveurs ou abritant du matériel « informatique ».

4.2.3.3 Liens entre biens essentiels et biens supports

Il s'agit d'établir le rapport existant entre les biens essentiels et les biens supports afin de mettre en évidence une gradation dans leur prise en charge sécuritaire. Dans le tableau 4.11 page suivante, on peut se rendre compte que, mis à part les logiciels embarqués qui ont peu de rapport avec le dossier administratif, le dossier médical ou le dossier infirmier, tous les biens supports sont liés aux différentes parties du bien essentiel.

				Biens essentiels					
				Dossier administratif	Dossier médical	Dossier infirmier	Dossier urgences	Dossier radiologique	Dossier laboratoire
Biens supports	SYS	MAT	Les matériels pour les réseaux filaires	x	x	x	x	x	x
		MAT	Les matériels pour les réseaux wifi	x	x	x	x	x	x
		MAT	Les PC et serveurs	x	x	x	x	x	x
		MAT	Les solutions de stockage	x	x	x	x	x	x
		RSX	Les réseaux filaires	x	x	x	x	x	x
		RSX	Les réseaux wifi	x	x	x	x	x	x
		LOG	Les SGBD	x	x	x	x	x	x
		LOG	Les applications	x	x	x	x	x	x
		LOG	Les systèmes d'exploitation	x	x	x	x	x	x
		LOG	Les logiciels embarqués				x	x	x
	ORG	PAP	Les documents imprimés	x	x	x	x	x	x
		CAN	Les discussions inter-personnelles	x	x	x	x	x	x
		PER	Les fonctions du personnel	x	x	x	x	x	x
	LOC	LOC	Les locaux informatiques	x	x	x	x	x	x

TABLE 4.11 – **Liens entre biens**

4.2.3.4 Mesures de sécurité existantes

Cette partie répertorie les mesures de sécurité existantes au sein de l'institution. Nous pourrons y mettre en évidence, en premier lieu, la redondance de différents éléments constitutifs du système d'information afin de pallier à une défaillance unique et, en second lieu, une séparation dans la localisation de ces différents éléments, afin de minimiser les risques de défaillances multiples.
Notre travail n'étudiant pas un hôpital précis, nous nous limiterons à citer des mesures communément appliquées :

- déploiement d'un antivirus,
- mise en place de procédure de sauvegarde,
- redondance du matériel réseau,
- redondance des bases de données,
- contrôle des accès aux applications,
- sécurisation du réseau en différents segments,
- sécurisation des locaux informatiques (point de vue feu, accès ...),
- limitation des accès extérieurs vers le réseau,
- sécurisation du réseau wifi (non-diffusion du SSID, clé de cryptage, ...),

– politique de confidentialité des impressions papier,
– contrat de maintenance sur les applications essentielles,
– procédure de destruction du matériel usagé (disque dur, bande de sauvegarde,...),
– ...

4.3 Module 2 : Etude des événements redoutés

4.3.1 Apprécier les événements redoutés

« *Cette activité fait partie de l'appréciation des risques. Elle a pour but de faire émerger et de caractériser les événements liés à la sécurité de l'information que l'organisme redoute, sans étudier la manière dont ceux-ci peuvent arriver. Elle permet également de fournir les éléments nécessaires au choix de traitement des risques afférents et à la définition des priorités de traitement.* » [ANS10b]

4.3.1.1 Analyse des événements redoutés

Dans les tableaux suivants (4.12 page suivante, 4.13 page 43, 4.14 page 44, 4.15 page 45, 4.16 page 45), le bien que nous avons défini comme essentiel, le dossier patient, est décomposé en ses constituants principaux [2] afin d'analyser les événements redoutés en rapport avec le besoin de sécurité de chacun d'entre eux.

Dans la première partie des tableaux, pour chaque événement redouté, nous verrons les sources de menaces et les impacts qu'elles peuvent avoir sur les biens essentiels.
Ces sources et leurs impacts sont communs à l'ensemble des parties du dossier patient, sans distinction du système sous-jacent, qu'il soit administratif ou autre.
La dernière partie du tableau reprend pour chaque bien essentiel, son niveau de besoin, ainsi que le degré de gravité que représente l'atteinte engendrée par l'événement redouté.

2. Dossier administratif : DA, Dossier médical : DM, Dossier infirmier : DI, Dossier radiologique : DR, Dossier du laboratoire : DL

Evénement redouté :	**Indisponibilité des données**
Sources des menaces	Problème réseau Vol de matériel Curiosité du patient, des visiteurs Malveillance interne ou externe Catastrophe Panne machine Incompétence, manque de formation
Impacts	Impossibilité de créer des admissions Difficulté majeure pour la prise en charge du patient par manque d'information sur le « passé » médical du patient Difficulté importante pour consulter l'antériorité des documents radiologiques et/ou des documents de laboratoire

Biens essentiels	Besoin en disponibilité	Niveau de gravité
DA	3	3
DM	4	3
DI	4	3
DR	3	3
DL	3	3

TABLE 4.12 – **Analyse des événements redoutés sur la disponibilité**

Evénement redouté :	**Altération des données**
Sources des menaces	Malveillance interne ou externe Usurpation d'identité Piratage du réseau Incompétence, manque de formation
Impacts	Mauvaise référence concernant un patient dans l'ensemble des dossiers Responsabilité engagée sur les plans éthiques et légaux Prise en charge erronée d'un patient

Biens essentiels	Besoin en disponibilité	Niveau de gravité
DA	3	3
DM	4	4
DI	4	4
DR	4	4
DL	4	4

TABLE 4.13 – **Analyse des événements redoutés sur l'intégrité des données**

Evénement redouté :	**Compromission des données**
Sources des menaces	Indiscrétion du personnel Curiosité de la part des patients, des visiteurs Usurpation d'identité Détournement des traces papiers Firme extérieure peu scrupuleuse Défaillance d'un organisme étatique Non-respect des procédures Piratage du réseau
Impacts	Responsabilité engagée sur les plans éthiques et légaux

Biens essentiels	Besoin en disponibilité	Niveau de gravité
DA	1	4
DM	4-3-1	4
DI	3	4
DR	2	4
DL	2	4

TABLE 4.14 – **Analyse des événements redoutés sur la confidentialité des données**

Evénement redouté :	**Accès non autorisé**
Sources des menaces	Firme extérieure peu fiable Curiosité de la part des patients, des visiteurs Traces papiers Personnel mal-intentionné Non-respect des procédures
Impacts	Responsabilité engagée sur les plans éthiques et légaux

Biens essentiels	Besoin en disponibilité	Niveau de gravité
DA	2	4
DM	3	4
DI	3	4
DR	3	4
DL	3	4

TABLE 4.15 – **Analyse des événements redoutés sur l'authentification**

Evénement redouté :	**Non imputabilité des actions**
Sources des menaces	Applications non conformes aux exigences Firme extérieure peu fiable Personnel mal-intentionné Non-respect des procédures
Impacts	Responsabilité engagée sur les plans éthiques et légaux

Biens essentiels	Besoin en disponibilité	Niveau de gravité
DA	2	2
DM	3	4
DI	3	4
DR	3	4
DL	3	4

TABLE 4.16 – **Analyse des événements redoutés sur la traçabilité**

4.3.1.2 Evaluation des événements redoutés

Cette étape fera, elle aussi, l'objet d'un consensus entre les différentes parties prenantes et permettra de hiérarchiser les événements redoutés sur base de leur gravité. Le but étant de pouvoir visualiser clairement les événements que l'institution estime devoir empêcher en priorité, à savoir ceux d'un niveau 4 ou 3, et les événements d'un niveau 0 ou 1 qu'elle pense pouvoir traiter ultérieurement(Cfr table 4.17).

Gravité	Evénements redoutés
4	– Compromission des données administratives, – Accès non autorisé aux données administratives, – Altération des données médicales, – Compromission des données médicales, – Accès non autorisé aux données médicales, – Non imputabilité des actions sur les données médicales, – Altération des données infirmières, – Compromission des données infirmières, – Accès non autorisé aux données infirmières, – Non imputabilité des actions sur les données infirmières, – Altération des données radiologiques, – Compromission des données radiologiques, – Accès non autorisé aux données radiologiques, – Non imputabilité des actions sur les données radiologiques, – Altération des données du laboratoire, – Compromission des données du laboratoire, – Accès non autorisé aux données du laboratoire, – Non imputabilité des actions sur les données du laboratoire.
3	– Indisponibilité des données administratives, – Altération des données administratives, – Indisponibilité des données médicales, – Indisponibilité des données infirmières, – Indisponibilité des données radiologiques, – Indisponibilité des données du laboratoire.
2	– Non imputabilité des actions sur les données administratives.
1	

TABLE 4.17 – **Classement des événements redoutés**

Le classement ainsi établi permet de mettre en évidence que la scission du dossier patient en différents sous-dossiers, pourra être abandonnée pour certains items et que la suite du travail pourra se faire de manière commune pour certains événements redoutés. Le tableau 4.17 page précédente peut donc se résumer en une deuxième version dans le tableau 4.18.

Gravité	Evénements redoutés
4	– Compromission des données du dossier patient, – Accès non autorisé aux données du dossier patient, – Altération des données médicales, infirmières, radiologiques ou du laboratoire, – Non imputabilité des actions sur les données médicales, infirmières, radiologiques ou du laboratoire.
3	– Indisponibilité des données du dossier patient, – Altération des données administratives.
2	– Non imputabilité des actions sur les données administratives.

TABLE 4.18 – **Classement combiné des événements redoutés**

4.4 Module 3 : Etude des scénarii de menaces

4.4.1 Apprécier les scénarii de menaces

« *Cette activité fait partie de l'appréciation des risques. Elle a pour but d'identifier les différentes possibilités d'actions sur les biens supports, afin de disposer d'une liste complète de scénarios de menaces. Elle permet également de fournir les éléments nécessaires au choix de traitement des risques afférents et à la définition des priorités de traitement.* » [ANS10b]

4.4.1.1 Analyse des scénarii de menaces

Les analyses de scénarii sont réalisées sur base d'interviews des différentes parties prenantes. Leur degré de vraisemblance sera estimé en tenant compte des vulnérabilités exposées par chaque bien support et sans tenir compte des mesures de sécurité qui auraient déjà été mises en place.

Le tableau suivant (Cfr table 4.19) présente les différents scénarii retrouvés en milieu hospitalier en distinguant pour chacun d'eux les impacts sur les domaines présentés dans le chapitre 3 page 21.
Les sources de menaces communément rencontrées sont données à titre d'exemples.

Impacts	Sources des menaces	Vraisemblance
SYS - Menaces sur le réseau filaire		
Maintenance du matériel, Surexploitation de la bande passante (téléchargement), Vol, Dégradation, destruction des câbles, Panne électrique.	Indisponibilité	3
Surexploitation de la bande passante (téléchargement), Intégration d'une machine licite dans le réseau.	Altération	3
Acquisition de données par écoute passive, Attaque « man in the middle ».	Compromission	2
Attaque « man in the middle ».	Défaut d'authentification	1
Attaque « man in the middle ».	Défaut de traçabilité	1
SYS - Le réseau wifi		
Maintenance du matériel, Vol, Panne électrique.	Indisponibilité	4
Surexploitation de la bande passante, Intégration d'une machine licite dans le réseau.	Altération	3
Acquisition de données par écoute passive, Attaque « man in the middle ».	Compromission	2
Attaque « man in the middle »..	Défaut d'authentification	1
Attaque « man in the middle ».	Défaut de traçabilité	1

Suite page suivante

Impacts	Sources des menaces	Vraisemblance
SYS - Les PC et serveurs		
Maintenance du matériel, Usure, dégradation du matériel, vol, Branchement de périphériques incompatibles, Panne électrique, court-circuit, incendie.	Indisponibilité	4
Surexploitation de l'alimentation électrique, panne électrique.	Altération	2
Maintenance du matériel, Vol, recyclage de matériel, Utilisation de matériels inappropriés à la sensibilité des informations stockées, Observation des écrans.	Compromission	3
Utilisation de matériels inappropriés à la sensibilité des informations stockées.	Défaut d'authentification	2
Surexploitation des capacités de traitement, Vol.	Défaut de traçabilité	3
SYS - Le stockage		
Surexploitation des capacités de stockage, Maintenance du matériel, Vieillissement du matériel, Vol, Incendie, Panne électrique.	Indisponibilité	4
Maintenance du matériel, Usure du matériel, Panne électrique.	Altération	4
Vol, Utilisation de matériels inappropriés à la sensibilité des informations stockées.	Compromission	2
Utilisation de matériels inappropriés à la sensibilité des informations stockées, Maintenance du matériel.	Défaut d'authentification	2
Utilisation de matériels inappropriés à la sensibilité des informations stockées, Maintenance du matériel, Panne électrique.	Défaut de traçabilité	3

Suite page suivante

Impacts	Sources des menaces	Vraisemblance
SYS - Les bases de données		
Maintenance du matériel, Effacement d'enregistrements, Surcharge de sessions, Incident électrique.	Indisponibilité	4
Incident électrique.	Altération	4
Procédure de backup non sécurisée, Maintenance du matériel, Elévation des privilèges d'un utilisateur.	Compromission	4
Elévation des privilèges d'un utilisateur.	Défaut d'authentification	2
Procédure de backup non sécurisée, Maintenance du matériel, Effacement d'enregistrements.	Défaut de traçabilité	4
SYS - Les applications		
Détournement de l'usage normal, Effacement d'exécutables, Manipulation inopportune, Changement de paramétrage.	Indisponibilité	4
Détournement de l'usage normal, Manipulation inopportune, Changement de paramétrage.	Altération	4
Manipulation inopportune, Détournement de l'usage normal, Elévation des privilèges d'un utilisateur.	Compromission	4
Elévation des privilèges d'un utilisateur.	Défaut d'authentification	3
Manipulation inopportune, Elévation des privilèges d'un utilisateur.	Défaut de traçabilité	4
SYS - Les systèmes d'exploitation		
Mise à jour inopportune, Panne électrique.	Indisponibilité	4
Mise à jour inopportune.	Altération	1
Mise à jour inopportune.	Compromission	1
Mise à jour inopportune.	Défaut d'authentification	2
Mise à jour inopportune.	Défaut de traçabilité	1

Suite page suivante

Impacts	Sources des menaces	Vraisemblance
SYS - Les logiciels embarqués		
Maintenance du matériel, Incident électrique.	Indisponibilité	3
Manipulation inopportune, Incident électrique.	Altération	3
Observation externe	Compromission	2
Manipulation inopportune, Elévation des privilèges d'un utilisateur.	Défaut d'authentification	2
Manipulation inopportune, Elévation des privilèges d'un utilisateur.	Défaut de traçabilité	2
ORG - Les documents imprimés		
Perte.	Indisponibilité	1
Falsification, Détérioration.	Altération	2
Perte, Réemploi pour un usage de brouillon.	Compromission	4
Perte.	Défaut d'authentification	4
Perte.	Défaut de traçabilité	4
ORG - Les discussions interpersonnelles		
Départ d'une personne.	Indisponibilité	1
Modification du contenu d'une transmission orale.	Altération	4
Divulgation involontaire, Corruption, manipulation.	Compromission	4
Ecoute de conversation, Corruption, manipulation.	Défaut d'authentification	4
Absence totale de traces.	Défaut de traçabilité	4

Suite page suivante

Impacts	Sources des menaces	Vraisemblance
ORG - Les fonctions du personnel		
Départ, Réorganisation hiérarchique.	Indisponibilité	2
Départ, Réorganisation hiérarchique.	Altération	2
Départ, Réorganisation hiérarchique.	Compromission	3
Mauvaise affectation des sécurités de groupe, de fonction.	Défaut d'authentification	4
Mauvaise affectation des sécurités de groupe, de fonction.	Défaut de traçabilité	3
LOC - Les locaux informatiques		
Incident, Accident.	Indisponibilité	3
Vandalisme.	Altération	2
Vandalisme.	Compromission	2
Entrée « par effraction ».	Défaut d'authentification	1
Entrée « par effraction ».	Défaut de traçabilité	1

TABLE 4.19 – **Analyse des scénarii de menaces**

4.4.1.2 Evaluation des scénarii de menaces

Le tableau récapitulatif (Cfr Table 4.20 page 54) permet de mettre en évidence une hiérarchie des vraisemblances dans les scénarii.
Celle-ci sera à l'intérieur de chaque classe, établie une fois de plus, par consensus entre les différentes parties prenantes. Ensuite, l'institution décidera de ce qu'elle prendra en compte en priorité.

Vraisemblance	Scénarii de menaces
4	Menaces sur le réseau wifi causant une indisponibilité
	Menaces sur le stockage causant une altération
	Menaces sur le stockage causant une indisponibilité
	Menaces sur les applications causant un défaut de traçabilité
	Menaces sur les applications causant une altération
	Menaces sur les applications causant une compromission
	Menaces sur les applications causant une indisponibilité
	Menaces sur les bases de données causant un défaut de traçabilité
	Menaces sur les bases de données causant une altération
	Menaces sur les bases de données causant une compromission
	Menaces sur les bases de données causant une indisponibilité
	Menaces sur les discussions interpersonnelles causant un défaut de traçabilité
	Menaces sur les discussions interpersonnelles causant un défaut d'authentification
	Menaces sur les discussions interpersonnelles causant une altération
	Menaces sur les discussions interpersonnelles causant une compromission
	Menaces sur les documents imprimés causant un défaut d'authentification
	Menaces sur les documents imprimés causant un défaut de traçabilité
	Menaces sur les documents imprimés causant une compromission
	Menaces sur les fonctions du personnel causant un défaut d'authentification
	Menaces sur les PC et serveurs causant une indisponibilité
	Menaces sur les systèmes d'exploitation causant une indisponibilité
3	Menaces sur le réseau filaire causant une altération
	Menaces sur le réseau filaire causant une indisponibilité
	Menaces sur le réseau wifi causant une altération
	Menaces sur le stockage causant un défaut de traçabilité
	Menaces sur les applications causant un défaut d'authentification
	Menaces sur les fonctions du personnel causant un défaut de traçabilité
	Menaces sur les fonctions du personnel causant une compromission
	Menaces sur les locaux informatiques causant une indisponibilité
	Menaces sur les logiciels embarqués causant une altération
	Menaces sur les logiciels embarqués causant une indisponibilité
	Menaces sur les PC et serveurs causant un défaut de traçabilité
	Menaces sur les PC et serveurs causant une compromission

Suite page suivante

Vraisemblance	Scénarii de menaces
2	Menaces sur le réseau filaire causant une compromission
	Menaces sur le réseau wifi causant une compromission
	Menaces sur le stockage causant un défaut d'authentification
	Menaces sur le stockage causant une compromission
	Menaces sur les bases de données causant un défaut d'authentification
	Menaces sur les documents imprimés causant une altération
	Menaces sur les fonctions du personnel causant une altération
	Menaces sur les fonctions du personnel causant une indisponibilité
	Menaces sur les locaux informatiques causant une altération
	Menaces sur les locaux informatiques causant une compromission
	Menaces sur les logiciels embarqués causant un défaut d'authentification
	Menaces sur les logiciels embarqués causant un défaut de traçabilité
	Menaces sur les logiciels embarqués causant une compromission
	Menaces sur les PC et serveurs causant un défaut d'authentification
	Menaces sur les PC et serveurs causant une altération
	Menaces sur les systèmes d'exploitation causant un défaut d'authentification
1	Menaces sur le réseau filaire causant un défaut d'authentification
	Menaces sur le réseau filaire causant un défaut de traçabilité
	Menaces sur le réseau wifi causant un défaut d'authentification
	Menaces sur le réseau wifi causant un défaut de traçabilité
	Menaces sur les discussions interpersonnelles causant une indisponibilité
	Menaces sur les documents imprimés causant une indisponibilité
	Menaces sur les locaux informatiques causant un défaut d'authentification
	Menaces sur les locaux informatiques causant un défaut de traçabilité
	Menaces sur les systèmes d'exploitation causant un défaut de traçabilité
	Menaces sur les systèmes d'exploitation causant une altération
	Menaces sur les systèmes d'exploitation causant une compromission

TABLE 4.20 – **Hiérarchie des scénarii de menaces**

4.5 Module 4 : Etude des risques

4.5.1 Apprécier les risques

« *Cette activité fait partie de l'appréciation des risques. Elle a pour but de mettre en évidence et de caractériser les risques réels pesant sur le périmètre de l'étude.* » [ANS10b]

4.5.1.1 Analyse des risques

Un risque est caractérisé par un événement redouté et par tous les scénarii susceptibles de l'engendrer.
La corrélation entre les événements redoutés et les scénarii de menaces se traduit, dans l'analyse des risques, par la mise en relation du degré de gravité des premiers et du niveau de vraisemblance des seconds.
Chaque risque analysé devrait éventuellement voir ses deux niveaux adaptés en fonction des mesures de sécurité que l'institution aurait déjà mises en place.

Dans les différents tableaux présentés au module 2, nous avons scindé le dossier patient en ses différents composants afin d'évaluer le niveau de besoin requis et le facteur de gravité des différents événements redoutés.

Dans le module 3, par le biais du tableau 4.19 page 52, nous avons relevé les différents scénarii possibles, avec leurs impacts et niveaux de vraisemblance.

Au cours de cette étape, nous résumerons pour chacun des sept risques (Cfr table 4.18 page 47), le besoin de sécurité estimé ainsi que son degré de gravité si le besoin n'est pas atteint. Nous ferons de même avec les différents scénarii envisagés et leur degré de vraisemblance. La dernière partie mettra en évidence les niveaux de gravité et de vraisemblance du risque analysé.
Nous citerons ce qui se fait généralement dans les institutions hospitalières sans pour autant pouvoir nous en servir dans la réévaluation des degrés de gravité et de vraisemblance du fait de la grande disparité pouvant exister dans leur mise en exécution.
Si nous avions étudié une institution bien particulière nous aurions eu une révision de ces deux niveaux en regard des mesures de sécurité déjà actives ou en cours d'application.

1. **Compromission des données du dossier patient**
   - Les différents besoins en confidentialité des sous-dossiers varient de publique à confidentiel (de 1 à 4) en fonction de la nature des informations que le sous-dossier gère, mais le degré de gravité en cas de non atteinte du besoin est toujours d'un niveau majeur (4) (Cfr table 4.14 page 44).
   - Les vraisemblances et l'intitulé des différents scénarii de menaces sont suivant le tableau 4.20 page précédente :

     Vraisemblance 4 : Menaces sur les bases de données

     Vraisemblance 4 : Menaces sur les applications

     Vraisemblance 4 : Menaces sur les documents imprimés

     Vraisemblance 4 : Menaces sur les discussions interpersonnelles

     Vraisemblance 3 : Menaces sur les fonctions du personnel

     Vraisemblance 3 : Menaces sur les PC et serveurs

Vraisemblance 2 : Menaces sur le stockage

Vraisemblance 2 : Menaces sur le réseau wifi

Vraisemblance 2 : Menaces sur le réseau filaire

Vraisemblance 2 : Menaces sur les logiciels embarqués

Vraisemblance 2 : Menaces sur les locaux informatiques

Vraisemblance 1 : Menaces sur les systèmes d'exploitation

- De nombreuses mesures existent déjà de manière intégrée au niveau des bases de données et des applications couramment employées au sein des hôpitaux. De la même manière, de nombreuses procédures, liées au secret professionnel, sont souvent mises en place, afin d'éviter l'ouverture de brêches dans la confidentialité des données.
- Niveaux globaux du risque :

  Gravité : 4

  Vraisemblance : 3

2. **Accès non autorisé aux données du dossier patient**
   - Les différents besoins en matière d'authentification sont soit un besoin en authentification basé sur des rôles, soit une authentification personnelle (2 ou 3) en fonction de la nature des informations que le sous-dossier gère, mais le degré de gravité en cas de non atteinte du besoin est toujours d'un niveau majeur (4) (Cfr table 4.15 page 45).
   - Les vraisemblances et l'intitulé des différents scénarii de menaces sont suivant le tableau 4.20 page 54 :

     Vraisemblance 4 : Menaces sur les documents imprimés

     Vraisemblance 4 : Menaces sur les discussions interpersonnelles

     Vraisemblance 4 : Menaces sur les fonctions du personnel

     Vraisemblance 3 : Menaces sur les applications

     Vraisemblance 2 : Menaces sur les PC et serveurs

     Vraisemblance 2 : Menaces sur le stockage

     Vraisemblance 2 : Menaces sur les bases de données

     Vraisemblance 2 : Menaces sur les logiciels embarqués

     Vraisemblance 2 : Menaces sur les systèmes d'exploitation

     Vraisemblance 1 : Menaces sur le réseau wifi

     Vraisemblance 1 : Menaces sur le réseau filaire

     Vraisemblance 1 : Menaces sur les locaux informatiques
   - De manière générale, les procédures et le respect strict du secret professionnel tel que cela est déjà mis en place dans les institutions hospitalières, permettent déjà de réduire la vraisemblance des scénarii. Il en est de même si les applications sont conçues de manière sécurisée.

- Niveaux globaux du risque :

  Gravité : 4

  Vraisemblance : 2

3. **Altération des données médicales, infirmières, radiologiques ou du laboratoire**
   - Les différents besoins en intégrité des sous-dossiers varient d'une récupération des données corrompues à une conservation complète de l'intégrité (de 3 à 4) en fonction de la nature des informations que le sous-dossier gère, mais le degré de gravité en cas de non atteinte du besoin est toujours d'un niveau majeure (4) (Cfr table 4.13 page 43).
   - Les vraisemblances et l'intitulé des différents scénarii de menaces sont suivant le tableau 4.20 page 54 :

     Vraisemblance 4 : Menaces sur les bases de données

     Vraisemblance 4 : Menaces sur les applications

     Vraisemblance 4 : Menaces sur les discussions interpersonnelles

     Vraisemblance 4 : Menaces sur le stockage

     Vraisemblance 3 : Menaces sur le réseau wifi

     Vraisemblance 3 : Menaces sur le réseau filaire

     Vraisemblance 3 : Menaces sur les logiciels embarqués

     Vraisemblance 2 : Menaces sur les documents imprimés

     Vraisemblance 2 : Menaces sur les fonctions du personnel

     Vraisemblance 2 : Menaces sur les PC et serveurs

     Vraisemblance 2 : Menaces sur les locaux informatiques

     Vraisemblance 1 : Menaces sur les systèmes d'exploitation
   - De manière générale, les procédures et le respect strict du secret professionnel tel que déjà mis en place dans les institutions hospitalières permettent déjà de réduire la vraisemblance des scénarii. Il en est de même si les applications sont conçues de manière sécurisée et que les données qu'elles gèrent ne peuvent être modifiées que sous de fortes contraintes.
   - Niveaux globaux du risque :

     Gravité : 4

     Vraisemblance : 3

4. **Non imputabilité des actions sur les données médicales, infirmières, radiologiques ou du laboratoire**
   - Le besoin en traçabilité des sous-dossiers concernés est un besoin de traçabilité complète (3), et le degré de gravité en cas de non atteinte du besoin est toujours d'un niveau majeur (4) (Cfr table 4.16 page 45).
   - Les vraisemblances et l'intitulé des différents scénarii de menaces sont suivant le tableau 4.20 page 54 :

     Vraisemblance 4 : Menaces sur les bases de données

     Vraisemblance 4 : Menaces sur les applications

     Vraisemblance 4 : Menaces sur les documents imprimés

     Vraisemblance 4 : Menaces sur les discussions interpersonnelles

     Vraisemblance 3 : Menaces sur les fonctions du personnel

     Vraisemblance 3 : Menaces sur les PC et serveurs

     Vraisemblance 3 : Menaces sur le stockage

     Vraisemblance 2 : Menaces sur les logiciels embarqués

     Vraisemblance 1 : Menaces sur le réseau wifi

     Vraisemblance 1 : Menaces sur le réseau filaire

     Vraisemblance 1 : Menaces sur les locaux informatiques

     Vraisemblance 1 : Menaces sur les systèmes d'exploitation
   - De manière générale, les procédures et le respect strict du secret professionnel tel que déjà mis en place dans les institutions hospitalières permettent déjà de réduire la vraisemblance des scénarii. Il en est de même si les applications sont conçues de manière sécurisée. De plus en plus, on parle également de l'horodatage des données que les applications doivent permettre.
   - Niveaux globaux du risque :

     Gravité : 4

     Vraisemblance : 3

5. **Indisponibilité des données du dossier patient**
   - Les différents besoins en disponibilité des sous-dossiers varient de très disponibles à hautement disponibles (3 ou 4) en fonction de la nature des informations que le sous-dossier gère, mais le degré de gravité en cas de non atteinte du besoin est toujours d'un niveau important (3) (Cfr table 4.12 page 42).
   - Les vraisemblances et l'intitulé des différents scénarii de menaces sont suivant le tableau 4.20 page 54 :

     Vraisemblance 4 : Menaces sur les bases de données

Vraisemblance 4 : Menaces sur les applications

Vraisemblance 1 : Menaces sur les documents imprimés

Vraisemblance 1 : Menaces sur les discussions interpersonnelles

Vraisemblance 2 : Menaces sur les fonctions du personnel

Vraisemblance 4 : Menaces sur les PC et serveurs

Vraisemblance 4 : Menaces sur le stockage

Vraisemblance 4 : Menaces sur le réseau wifi

Vraisemblance 3 : Menaces sur le réseau filaire

Vraisemblance 3 : Menaces sur les logiciels embarqués

Vraisemblance 3 : Menaces sur les locaux informatiques

Vraisemblance 4 : Menaces sur les systèmes d'exploitation

- Face à ce besoin, qui s'avère bien souvent important aux yeux des utilisateurs en regard des données et de leurs implications dans la prise en charge des patients, de nombreuses mesures existent et sont mises en place (redondance des différents matériels utilisés, duplication des bases de données, procédure de secours pour pallier aux pannes, ...). Ces mesures ne sont pas toujours appliquées partout avec la même efficience.
- Niveaux globaux du risque :

  Gravité : 3

  Vraisemblance : 4

6. **Altération des données administratives**
   - Le besoin en intégrité du sous-dossier concerné est la récupération des données éventuellement corrompues (3) en fonction de la nature des informations que le sous-dossier gère, mais le degré de gravité en cas de non atteinte du besoin est d'un niveau important (3) (Cfr table 4.13 page 43).
   - Les vraisemblances et l'intitulé des différents scénarii de menaces sont suivant le tableau 4.20 page 54 :

     Vraisemblance 4 : Menaces sur les bases de données

     Vraisemblance 4 : Menaces sur les applications

     Vraisemblance 4 : Menaces sur les discussions interpersonnelles

     Vraisemblance 4 : Menaces sur le stockage

     Vraisemblance 3 : Menaces sur le réseau wifi

     Vraisemblance 3 : Menaces sur le réseau filaire

     Vraisemblance 3 : Menaces sur les logiciels embarqués

     Vraisemblance 2 : Menaces sur les documents imprimés

Vraisemblance 2 : Menaces sur les fonctions du personnel

Vraisemblance 2 : Menaces sur les PC et serveurs

Vraisemblance 2 : Menaces sur les locaux informatiques

Vraisemblance 1 : Menaces sur les systèmes d'exploitation

- De manière générale, les procédures et le respect strict du secret professionnel tel que déjà mis en place dans les institutions hospitalières permettent déjà de réduire la vraisemblance des scénarii. Il en est de même si les applications sont conçues de manière sécurisée et que les données qu'elles gèrent ne peuvent être modifiées que sous de fortes contraintes.
- Niveaux globaux du risque :

  Gravité : 3

  Vraisemblance : 3

7. **Non imputabilité des actions sur les données administratives**
   - Le besoin en traçabilité du dossier administratif est d'avoir une traçabilité d'un niveau incomplet (2) en fonction de la nature des informations que le sous-dossier gère, et le degré de gravité en cas de non atteinte du besoin est d'un niveau négligeable (2) (Cfr table 4.16 page 45).
   - Les vraisemblances et l'intitulé des différents scénarii de menaces sont suivant le tableau 4.20 page 54 :

     Vraisemblance 4 : Menaces sur les bases de données

     Vraisemblance 4 : Menaces sur les applications

     Vraisemblance 4 : Menaces sur les documents imprimés

     Vraisemblance 4 : Menaces sur les discussions interpersonnelles

     Vraisemblance 3 : Menaces sur les fonctions du personnel

     Vraisemblance 3 : Menaces sur les PC et serveurs

     Vraisemblance 3 : Menaces sur le stockage

     Vraisemblance 2 : Menaces sur les logiciels embarqués

     Vraisemblance 1 : Menaces sur le réseau wifi

     Vraisemblance 1 : Menaces sur le réseau filaire

     Vraisemblance 1 : Menaces sur les locaux informatiques

     Vraisemblance 1 : Menaces sur les systèmes d'exploitation
   - De manière générale, les procédures et le respect strict du secret professionnel tel que déjà mis en place dans les institutions hospitalières permettent déjà de réduire la vraisemblance des scénarii. Il en est de même si les applications sont conçues de manière sécurisée. De plus en plus, on parle également de l'horodatage des données que les applications doivent permettre..

- Niveaux globaux du risque :

  Gravité : 2

  Vraisemblance : 3

4.5.1.2 Evaluation des risques

Suite à l'analyse de la gravité des risques et de la vraisemblance des scénarii envisagés, et avec l'aide du tableau 4.10 page 38, nous constituons le tableau 4.21 dans lequel nous mettons en évidence six risques dans la zone des risques intolérables. Il est nécessaire de les traiter ; ce sont, par ordre d'importance et en lien avec les numéros de l'étape antérieure les risques : 1-3-4-5-6-2.
Un risque, le risque 7, se trouve dans la zone des risques significatifs, il est facultatif de le traiter dans l'immédiat. Par contre, nous n'avons pas de risques négligeables.

Dans l'étude d'une institution précise, nous pourrions, sur base des mesures déjà activées, réévaluer la gravité des risques et la vraisemblance des scénarii, ce qui conduirait à une réorganisation de la table.

4.5.2 Identifier les objectifs de sécurité

« *Cette activité fait partie du traitement des risques. Elle a pour but de choisir la manière dont chaque risque devra être traité au regard de son évaluation.* » [ANS10b]

4.5.2.1 Choix des options de traitements des risques

A ce niveau, l'institution, évaluant les risques courus par son Système d'information, doit définir les objectifs de sécurité qui vont la guider dans le traitement des risques auxquels elle estime ne pas pouvoir se soumettre. Ces objectifs sont, typiquement de quatre ordres :

- Evitement : le risque est insupportable pour l'institution, les scenarii pouvant amener le risque doivent être supprimés pour que le risque ne se produise pas.
- Réduction : le risque continue d'être pris, mais ses conséquences doivent être réduites afin d'impacter le moins possible l'institution.
- Prise : le risque est négligeable et/ou son traitement peut être reporté à plus tard.
- Transfert : le risque doit être transféré vers une autre institution plus à même de le gérer ou d'en assurer les conséquences (sous-traitant, assurance, ...).

Gravité	4		2. Accès non autorisé aux données du dossier patient	1. Compromission des données du dossier patient 3. Altération des données médicales, infirmières, radiologiques ou du laboratoire 4. Non imputabilité des actions sur les données médicales, infirmières, radiologiques ou du laboratoire	
	3			6. Altération des données administratives	5. Indisponibilité des données du dossier patient
	2			7. Non imputabilité des actions sur les données administratives	
	1				
		1	2	3	4
		Vraisemblance			

TABLE 4.21 – **Evaluation des risques relevés**

Le tableau (Cfr table 4.22 page suivante) reprend les sept risques étudiés avec pour chacun d'eux l'objectif de sécurité qui devrait être poursuivi sachant que plusieurs choix de traitement sont possibles.

On observe que pour l'ensemble des risques étudiés, ceux-ci doivent être évités ou réduits, ce qui correspond bien aux exigences légales évoquées dans le premier chapitre. Les deux possibilités de transfert pourraient se concrétiser dans la souscription à une assurance couvrant les conséquences d'un défaut de sécurisation.

4.5.2.2 Risques résiduels

De l'ensemble des risques étudiés, nous pensons qu'un seul risque (Cfr table 4.23 page suivante) pourrait être laissé de côté et être traité comme un risque résiduel pris en compte ultérieurement quand les six autres auront été traités.
Dans les faits, les mesures de sécurité qui seront mises en œuvre pour traiter les risques intolérables, pourraient également avoir un impact de correction des niveaux de ce risque résiduel, à tel point, qu'il pourrait se trouver annihiler.

Risque	Evitement	Réduction	Prise	Transfert
1. Compromission des données du dossier patient	X			(X)
2. Accès non autorisé aux données du dossier patient	X	X		
3. Altération des données médicales, infirmières, radiologiques ou du laboratoire	X	X		(X)
4. Non imputabilité des actions sur les données médicales, infirmières, radiologiques ou du laboratoire	X	X		
5. Indisponibilité des données du dossier patient	X	X		
6. Altération des données administratives	X	X		
7. Non imputabilité des actions sur les données administratives		X	X	

TABLE 4.22 – **Table de choix du traitement des risques**

Risque résiduel	7. Non imputabilité des actions sur les données administratives
Gravité	Niveau 2 : la gravité est négligeable : la sécurité du dossier patient est compromise. Des données concernant un patient sont susceptibles d'être diffusées dans l'hôpital, parmi du personnel soumis au secret professionnel, mais ne prenant pas en charge ce patient
Vraisemblance	Niveau 3 : la menace va probablement se produire si certains facteurs sont réunis

TABLE 4.23 – **Risque résiduel**

4.6 Module 5 : Etude des mesures de sécurité

4.6.1 Formaliser les mesures de sécurité

« *Cette activité fait partie du traitement des risques. Elle a pour but de déterminer les mesures de sécurité adéquates pour atteindre les objectifs de sécurité identifiés, d'identifier les risques résiduels et de valider "formellement" les choix effectués.* » [ANS10b]

4.6.1.1 Déterminer les mesures de sécurité

Pour la détermination des mesures de sécurité, nous nous référerons aux normes ISO 27001 [3][27005a], 27002 [4][27005b], 27005 [5][27005c].
Rappelons ici que ces normes ISO sont des normes internationales traitant du management de la sécurité des Systèmes d'Information. Tout organisme qui respecte ces exigences en matière de sécurité peut se faire certifier s'il le souhaite.
Dans l'annexe A de la norme ISO 27001 sont citées 133 mesures de sécurité réparties en 11 catégories (réparties en chapitres, de 5 à 15). Elles sont décrites de manière plus détaillée dans la norme ISO 27002.

Précisons ici, pour la compréhension des points suivants, que sous chaque titre « **Risques visés par la mesure** », le lecteur trouvera un tableau reprenant les six risques intolérables étudiés avec la numérotation suivante :

1. Compromission des données du dossier patient
2. Accès non autorisé aux données du dossier patient
3. Altération des données médicales, infirmières, radiologiques ou du laboratoire
4. Non imputabilité des actions sur les données médicales, infirmières, radiologiques ou du laboratoire
5. Indisponibilité des données du dossier patient
6. Altération des données administratives

La présentation du tableau ci-après

1	2		4	5	6

doit toujours être comprise comme suit : la mesure étudiée vise les risques 1, 2, 4, 5 et 6, elle ne cible pas le risque 3.

Les différentes mesures se sécurité proposées ci-après aux institutions hospitalières couvrent les différents thèmes des normes ISO.

3. ISO 27001 : Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences
4. ISO 27002 : code des bonnes pratiques pour la gestion de la sécurité de l'information
5. ISO 27005 : la première norme de gestion des risques de la Sécurité des Systèmes d'Information

1. **Politique de sécurité**

   (a) **Mesure de sécurité** :

   - La politique de sécurité de l'information est élaborée et diffusée après validation par la direction de l'institution

   Risques visés par la mesure :

1	2	3	4	5	6

   Bien support sur lequel porte la mesure :

   - ORG - Organisation de l'institution hospitalière

   Thème ISO 27002 :

   - 5.1. Politique de sécurité de l'information

   Types de mesure de sécurité :

   - Prévention
   - Protection
   - Récupération

   (b) **Mesure de sécurité** :

   - Une révision de la politique de sécurité de l'information, par l'ensemble des parties prenantes, est prévue à intervalle prédéterminé, mais aussi en cas de changement de législation ou d'infrastructures

   Risques visés par la mesure :

1	2	3	4	5	6

   Bien support sur lequel porte la mesure :

   - ORG - Organisation de l'institution hospitalière

   Thème ISO 27002 :

   - 5.1. Politique de sécurité de l'information

   Types de mesure de sécurité :

   - Prévention
   - Protection
   - Récupération

2. **Organisation de la sécurité de l'information**

(a) **Mesure de sécurité** :

- Il existe un soutien de la direction vis-à-vis de la sécurité de l'information, par le biais de directives, d'attribution de fonctions et de responsabilités dans la lutte contre les risques

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 6.1. Organisation interne

Types de mesure de sécurité :

- Prévention
- Protection
- Récupération

(b) **Mesure de sécurité** :

- La coordination des mesures est assurée par les responsables nommés

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 6.1. Organisation interne

Types de mesure de sécurité :

- Prévention
- Protection
- Récupération

(c) **Mesure de sécurité** :

- Les exigences légales et éthiques en matière de confidentialité et de secret professionnel sont clairement identifiées et actualisées

Risques visés par la mesure :

1	2	3	4		6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 6.1. Organisation interne

Type de mesure de sécurité :

- Prévention

(d) **Mesure de sécurité** :

- Les visiteurs et les sous-traitants sont systématiquement accompagnés dans les locaux sécurisés, après avoir enregistré leur présence et motif d'entrée

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 6.2. Tiers

Types de mesure de sécurité :

- Prévention
- Protection

(e) **Mesure de sécurité** :

- Lors de la signature de contrats, les clauses de confidentialité pour les sous-traitants et les firmes de maintenance sont présentes

Risques visés par la mesure :

1	2		4		

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 6.2. Tiers

Types de mesure de sécurité :

- Prévention
- Protection

3. **Gestion des biens**

(a) **Mesure de sécurité** :

- Un inventaire des biens sensibles de l'institution et de leurs gestionnaires est réalisé

Risques visés par la mesure :

1	2	3		5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 7.1. Responsabilités relatives aux biens

Types de mesure de sécurité :

- Prévention
- Protection
- Récupération

(b) **Mesure de sécurité** :

- A chaque nouveau matériel ou technologie mis en place, une diffusion interne des règles d'utilisation est prévue

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 7.1. Responsabilités relatives aux biens

Types de mesure de sécurité :

- Prévention
- Protection

(c) **Mesure de sécurité** :

- Le mode de traçabilité à mettre en œuvre pour chaque type d'information (sous-dossier) est clairement et précisément défini

Risques visés par la mesure :

1	2		4		

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 7.1. Responsabilités relatives aux biens

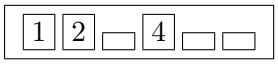
Type de mesure de sécurité :

- Prévention

(d) **Mesure de sécurité** :

- Les documents imprimés portent la marque « Confidentiel » ou « Réservé » en fonction du type de données qu'ils contiennent

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- PAP - Support papier

Thème ISO 27002 :

- 7.2. Classification des informations

Type de mesure de sécurité :

- Prévention

4. **Sécurité liée aux ressources humaines**

(a) **Mesure de sécurité** :

- Tout type de personnel signe une charte de respect de la confidentialité et une charte de responsabilisation dans l'utilisation de l'outil informatique

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 8.1. Avant le recrutement

Type de mesure de sécurité :

- Prévention

(b) **Mesure de sécurité** :

- Des campagnes d'information pour sensibiliser le personnel aux risques encourus sont régulièrement organisées

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- PER - Utilisateur

Thème ISO 27002 :

- 8.2. Pendant la durée du contrat

Type de mesure de sécurité :

- Prévention

(c) **Mesure de sécurité** :

- Le personnel est formé à l'usage sécurisé des applications et/ou matériels utilisés

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- PER - Utilisateur

Thème ISO 27002 :

- 8.2. Pendant la durée du contrat

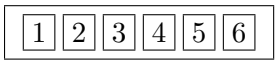
Types de mesure de sécurité :

- Prévention
- Protection

(d) **Mesure de sécurité** :

- Les mots de passe des firmes de maintenance sont limités à la durée minimale que leurs actions requièrent

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- PER - Utilisateur extérieur

Thème ISO 27002 :

- 8.2. Pendant la durée du contrat

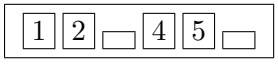
Type de mesure de sécurité :

- Prévention

(e) **Mesure de sécurité** :

- La notion de faute grave en cas d'atteinte à la confidentialité des données est inscrite dans le règlement de travail. Y figurent également les sanctions encourues

Risques visés par la mesure :



Biens supports sur lesquels porte la mesure :

- PER - Utilisateur
- CAN - Discussions inter-personnelles

Thème ISO 27002 :

- 8.2. Pendant la durée du contrat

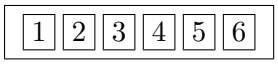
Type de mesure de sécurité :

- Prévention

(f) **Mesure de sécurité** :

- Lorsqu'un membre du personnel arrive à la fin de son contrat, ses droits d'accès (physiques et logiciels) sont immédiatement supprimés

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- PER - Utilisateur

Thème ISO 27002 :

- 8.3. Fin ou modification de contrat

Types de mesure de sécurité :

- Prévention
- Protection

(g) **Mesure de sécurité** :

- Lors du départ d'un membre du personnel disposant du/des mots de passe « administrateur », ceux-ci sont changés

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- PER - Administrateur

Thème ISO 27002 :

- 8.3. Fin ou modification de contrat

Types de mesure de sécurité :

- Prévention
- Protection

5. **Sécurité physique et environnementale**

(a) **Mesure de sécurité** :

- L'accès aux locaux informatiques ou recelant du matériel repris comme tel, est interdit à toute personne extérieure en-dehors de la présence d'un membre du personnel autorisé

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- LOC - Locaux de l'institution hospitalière

Thème ISO 27002 :

- 9.1. Zones sécurisées

Type de mesure de sécurité :

- Prévention

(b) **Mesure de sécurité** :

- Des dispositifs de lutte contre l'incendie sont mis en place dans les locaux informatiques critiques (salle « machines », salle de stockage , ...)

Risques visés par la mesure :

		3	4	5	6

Bien support sur lequel porte la mesure :

- LOC - Locaux de l'institution hospitalière

Thème ISO 27002 :

- 9.1. Zones sécurisées

Type de mesure de sécurité :

- Protection

(c) **Mesure de sécurité** :

- Des alarmes anti-intrusions sont installées dans les locaux informatiques critiques

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- LOC - Locaux de l'institution hospitalière

Thème ISO 27002 :

- 9.1. Zones sécurisées

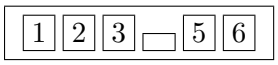
Types de mesure de sécurité :

- Prévention
- Protection

(d) **Mesure de sécurité** :

- Des consignes de fermeture à clef des locaux sont communiquées et imposées au personnel

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- LOC - Locaux de l'institution hospitalière

Thème ISO 27002 :

- 9.1. Zones sécurisées

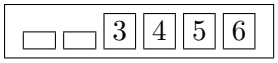
Types de mesure de sécurité :

- Prévention
- Protection

(e) **Mesure de sécurité** :

- Le matériel critique (serveur, équipement réseau, ...) est alimenté électriquement par plusieurs sources

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- MAT - Serveur réseau et machines

Thème ISO 27002 :

- 9.2. Sécurité du matériel

Types de mesure de sécurité :

- Prévention
- Protection

(f) **Mesure de sécurité** :

- Sur les écrans susceptibles d'être visualisés par des personnes extérieures, des films dits « de secret » sont apposés

Risques visés par la mesure :

Bien support sur lequel porte la mesure :

- MAT - Serveur réseau et machines

Thème ISO 27002 :

- 9.2. Sécurité du matériel

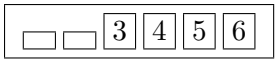
Types de mesure de sécurité :

- Prévention
- Récupération

(g) **Mesure de sécurité** :

- Une climatisation adéquate est installée dans les locaux informatiques critiques

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- LOC - Locaux de l'institution hospitalière

Thème ISO 27002 :

- 9.2. Sécurité du matériel

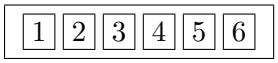
Type de mesure de sécurité :

- Prévention

(h) **Mesure de sécurité** :

- Des scellés sont installés sur les ordinateurs afin de pouvoir constater leur ouverture non désirée

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- MAT - Serveur réseau et machines

Thème ISO 27002 :

- 9.2. Sécurité du matériel

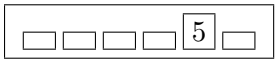
Type de mesure de sécurité :

- Prévention

(i) **Mesure de sécurité** :

- Des contrats de maintenance informatique sont souscrits afin de respecter les délais d'indisponibilité maximale désirée

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 9.2. Sécurité du matériel

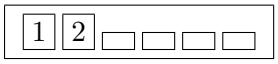
Types de mesure de sécurité :

- Prévention
- Récupération

(j) **Mesure de sécurité** :

- Tout équipement mis au rebut voit ses supports mémoires correctement effacés

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 9.2. Sécurité du matériel

Type de mesure de sécurité :

- Prévention

6. **Gestion de l'exploitation et des télécommunications**

(a) **Mesure de sécurité** :

- Il existe une documentation écrite de toutes les procédures d'exploitation existantes

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 10.1. Procédures et responsabilités liées à l'exploitation

Type de mesure de sécurité :

- Prévention

(b) **Mesure de sécurité** :

- Les composants inutiles des Systèmes d'exploitation sont désactivés et des procédures empêchant leurs modifications sans un accès dûment authentifié sont rédigées

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- LOG - Système d'exploitation

Thème ISO 27002 :

- 10.1. Procédures et responsabilités liées à l'exploitation

Type de mesure de sécurité :

- Prévention

(c) **Mesure de sécurité** :

- Un système de monitoring du parc informatique est organisé

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- MAT - Serveur réseau et machines

Thème ISO 27002 :

- 10.1. Procédures et responsabilités liées à l'exploitation

Types de mesure de sécurité :

- Prévention
- Récupération

(d) **Mesure de sécurité** :

- Un environnement de test permettant d'évaluer les changements logiciels ou matériels envisagés est prévu

Risques visés par la mesure :

1	2	3	4	5	6

Biens supports sur lesquels porte la mesure :

- MAT - Serveur réseau et machines
- LOG - Applications

Thème ISO 27002 :

- 10.1. Procédures et responsabilités liées à l'exploitation

Type de mesure de sécurité :

- Prévention

(e) **Mesure de sécurité** :

- Des rapports d'intervention sont exigés de la part des sociétés tierces intervenant sur le matériel ou les logiciels

Risques visés par la mesure :

1	2	3	4	5	6

Biens supports sur lesquels porte la mesure :

- MAT - Serveur réseau et machines
- LOG - Applications

Thème ISO 27002 :

- 10.2. Gestion de la prestation de service par un tiers

Types de mesure de sécurité :

- Protection
- Récupération

(f) **Mesure de sécurité** :

- Les ressources utilisées par les applications, les utilisateurs et les équipements sont surveillées

Risques visés par la mesure :

1	2	3	4	5	6

Biens supports sur lesquels porte la mesure :

- MAT - Serveur réseau et machines
- LOG - Applications
- PER - Utilisateurs

Thème ISO 27002 :

- 10.3. Planification et acceptation du système

Types de mesure de sécurité :

- Prévention
- Protection

(g) **Mesure de sécurité** :

- Un antivirus est installé et actualisé sur les différents Systèmes d'exploitation

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- LOG - Système d'exploitation

Thème ISO 27002 :

- 10.4. Protection contre les codes malveillants et mobiles

Type de mesure de sécurité :

- Protection

(h) **Mesure de sécurité** :

- Une sauvegarde « régulière » des applications et des données est réalisée, ce qui permet une récupération complète des informations

Risques visés par la mesure :

		3	4	5	6

Bien support sur lequel porte la mesure :

- LOG - Applications

Thème ISO 27002 :

- 10.5. Sauvegarde

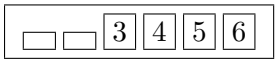
Type de mesure de sécurité :

- Récupération

(i) **Mesure de sécurité** :

- Des tests de restauration des données sauvegardées sont réalisés régulièrement afin de garantir la validité de l'ensemble de la procédure

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- LOG -Applications

Thème ISO 27002 :

- 10.5. Sauvegarde

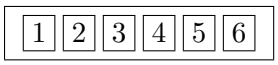
Types de mesure de sécurité :

- Prévention
- Récupération

(j) **Mesure de sécurité** :

- Une attention particulière est apportée à la sécurisation des équipements réseaux (dans leurs accès et dans la possibilité de s'y connecter), elle est renforcée pour le matériel Wifi (non diffusion du SSID, clé WPA2, ...)

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- MAT - Commutateur

Thème ISO 27002 :

- 10.6. Gestion de la sécurité des réseaux

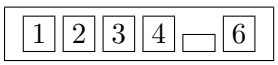
Type de mesure de sécurité :

- Prévention

(k) **Mesure de sécurité** :

- Tout type de supports amovibles est rangé dans un coffre ignifuge et est détruit complètement lors de leur mise au rebut

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- MAT - Matériel de sauvegarde

Thème ISO 27002 :

- 10.7. Manipulation des supports

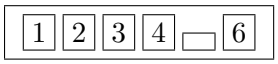
Types de mesure de sécurité :

- Prévention
- Récupération

(l) **Mesure de sécurité** :

- La consultation de ces supports amovibles fait l'objet de procédures écrites, gardant la trace des « visiteurs »

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 10.7. Manipulation des supports

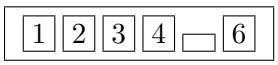
Types de mesure de sécurité :

- Prévention
- Récupération

(m) **Mesure de sécurité** :

- Des procédures d'échange (validité, modalités, ...) et de vérification des empreintes des fichiers échangés avec les institutions extérieures sont prévues

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- LOG - Serveurs logiciels du réseau interne

Thème ISO 27002 :

- 10.8. Echange d'informations

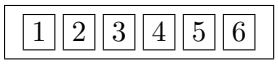
Type de mesure de sécurité :

- Protection

(n) **Mesure de sécurité** :

- Les événements informatiques (accès, erreurs, ...) sont journalisés et analysés afin d'en corriger les causes le plus rapidement possible

Risques visés par la mesure :



Biens supports sur lesquels porte la mesure :

- MAT - Matériel
- LOG - Applications
- LOC - Locaux informatiques

Thème ISO 27002 :

- 10.10. Surveillance

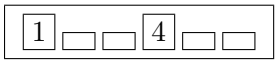
Types de mesure de sécurité :

- Protection
- Récupération

(o) **Mesure de sécurité** :

- Une procédure d'horodatage des actions entreprises sur les données existe

Risques visés par la mesure :



Biens supports sur lesquels porte la mesure :

- MAT - Matériel
- LOG - Applications

Thème ISO 27002 :

- 10.10. Surveillance

Types de mesure de sécurité :

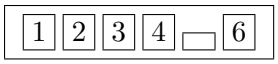
- Prévention
- Récupération

7. **Contrôle d'accès**

(a) **Mesure de sécurité** :

- Les droits d'accès des utilisateurs sont basés sur les fonctions des personnes. Ils doivent être réévalués face à tout changement applicatif ou lors de réaffectation de personnes. Ces droits font l'objet de documentations exhaustives

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thèmes ISO 27002 :

- 11.1. Exigences métier relatives au contrôle d'accès
- 11.2. Gestion de l'accès utilisateur

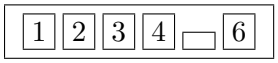
Type de mesure de sécurité :

- Prévention

(b) **Mesure de sécurité** :

- Les mots de passe font l'objet de procédures documentées quant à leur choix, de modification régulière et en tout cas à chaque suspicion de compromission

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- PER - Utilisateur

Thème ISO 27002 :

- 11.3. Responsabilités utilisateurs

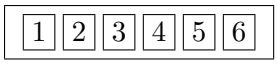
Type de mesure de sécurité :

- Prévention

(c) **Mesure de sécurité** :

- Les équipements informatiques non utilisés bénéficient d'un verrouillage systématique, manuel et/ou automatique

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- PER - Utilisateur

Thèmes ISO 27002 :

- 11.3. Responsabilités utilisateurs
- 11.5. Contrôle d'accès

Types de mesure de sécurité :

- Prévention
- Protection

(d) **Mesure de sécurité** :

- La gestion des droits d'accès est aussi restrictive que possible en ne donnant accès qu'aux services nécessaires

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- LOG - Serveurs logiciels du réseau interne

Thème ISO 27002 :

- 11.4. Contrôle d'accès au réseau

Types de mesure de sécurité :

- Prévention
- Protection

(e) **Mesure de sécurité** :

- La gestion du réseau permet une connexion fiable aux applications

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- LOG - Serveurs logiciels du réseau interne

Thème ISO 27002 :

- 11.4. Contrôle d'accès au réseau

Types de mesure de sécurité :

- Prévention
- Protection

(f) **Mesure de sécurité** :

- Dans la mesure du possible, l'identifiant et donc le mot de passe de l'utilisateur est géré de manière centrale (Active Directory, LDAP, ...)

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 11.5. Contrôle d'accès au système d'exploitation

Types de mesure de sécurité :

- Prévention
- Protection

(g) **Mesure de sécurité** :

- Les accès nécessaires pour la maintenance des différents systèmes sont aussi courts et restrictifs que nécessaire

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- MAT - PC et serveurs

Thème ISO 27002 :

- 11.6. Contrôle d'accès aux applications et à l'information

Types de mesure de sécurité :

- Prévention
- Protection

(h) **Mesure de sécurité** :

- Les systèmes identifiés comme sensibles disposent d'un environnement spécifique

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- MAT - Serveurs

Thème ISO 27002 :

- 11.6. Contrôle d'accès aux applications et à l'information

Type de mesure de sécurité :

- Prévention

(i) **Mesure de sécurité** :

- Une procédure claire est écrite pour la connexion et l'utilisation de matériel mobile (ordinateurs portables, PDA, ...)

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- MAT - Ordinateurs portables

Thème ISO 27002 :

- 11.7. Informatique mobile et télétravail

Type de mesure de sécurité :

- Protection

(j) **Mesure de sécurité** :

- Une procédure claire est rédigée pour la connexion et l'utilisation du télétravail

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 11.7. Informatique mobile et télétravail

Type de mesure de sécurité :

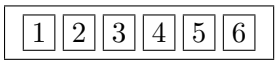
- Protection

8. **Acquisition, développement et maintenance des systèmes d'information**

(a) **Mesure de sécurité** :

- Le cahier des charges de toute nouvelle application prend en compte les exigences de sécurité et de confidentialité requises

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 12.1. Exigences de sécurité applicables aux systèmes d'information

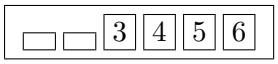
Type de mesure de sécurité :

- Prévention

(b) **Mesure de sécurité** :

- Les applications et/ou le système de base de données ont la responsabilité de vérifier la qualité des informations encodées

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 12.2. Bon fonctionnement des applications

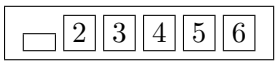
Types de mesure de sécurité :

- Prévention
- Protection

(c) **Mesure de sécurité** :

- Au minimum un système RAID, ou assimilé, est mis en place sur les serveurs. La redondance du réseau et des bases de données est instaurée

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- MAT - Serveurs

Thème ISO 27002 :

- 12.2. Bon fonctionnement des applications

Types de mesure de sécurité :

- Protection
- Récupération

(d) **Mesure de sécurité** :

- Une politique de mesures cryptographiques (chiffrement, création d'empreintes, ...) et/ou d'anonymisation efficace est mise en place pour les envois de données à l'extérieur de l'institution hospitalière

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thèmes ISO 27002 :

- 12.3. Mesures cryptographiques
- 12.4. Sécurité des fichiers

Type de mesure de sécurité :

- Prévention

(e) **Mesure de sécurité** :

- Toute modification d'applications, de matériel n'est implémentée qu'après une série de tests

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- LOG - Applications, PC et serveurs

Thème ISO 27002 :

- 12.6. Gestion des vulnérabilités

Types de mesure de sécurité :

- Prévention
- Protection

9. **Gestion des incidents liés à la sécurité de l'information**

(a) **Mesure de sécurité** :

- Tous les événements touchant la sécurité de l'information sont relatés, même et surtout s'ils sont le fait de firmes extérieures

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Sous-traitants

Thème ISO 27002 :

- 13.1. Signalement des événements et des failles liés à la sécurité de l'information

Types de mesure de sécurité :

- Protection
- Récupération

(b) **Mesure de sécurité** :

- Toutes les traces sont conservées conformément aux dispositions légales ou éthiques

Risques visés par la mesure :

1	2	3	4		6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 13.2. Gestion des améliorations et incidents liés à la sécurité de l'information

Type de mesure de sécurité :

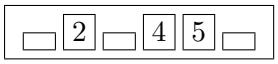
- Protection

10. **Gestion du plan de continuité de l'activité**

(a) **Mesure de sécurité** :

- Des plans de secours et de reprise sont établis pour les différentes applications et matériels critiques. Ces plans doivent se coordonner entre eux, les applications et/ou matériels étant souvent « interconnectés ». Les plans sont validés et testés de manière régulière afin de s'assurer de leur justesse face aux évolutions

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité

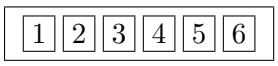
Type de mesure de sécurité :

- Récupération

(b) **Mesure de sécurité** :

- Les assurances nécessaires (altération ou compromission des données, vol, ...) sont contractées pour le personnel et pour le matériel

Risques visés par la mesure :



Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité

Type de mesure de sécurité :

- Récupération

11. **Conformité**

(a) **Mesure de sécurité** :

- Les exigences réglementaires sont être inventoriées et suivies de près

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 15.1. Conformité avec les exigences légales

Type de mesure de sécurité :

- Prévention

(b) **Mesure de sécurité** :

- L'application des procédures est vérifiée par les différents responsables

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 15.2. Conformité avec les politiques et normes de sécurité et conformité technique

Type de mesure de sécurité :

- Prévention

(c) **Mesure de sécurité** :

- Les différentes mesures de sécurité sont contrôlées de manière régulière et fixée à l'avance

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 15.3. Prises en compte de l'audit du système d'information

Types de mesure de sécurité :

- Prévention
- Protection

(d) **Mesure de sécurité** :

- Les différentes traces sont particulièrement surveillées et garanties contre toute modification ou effacement

Risques visés par la mesure :

1	2	3	4	5	6

Bien support sur lequel porte la mesure :

- ORG - Organisation de l'institution hospitalière

Thème ISO 27002 :

- 15.3. Prises en compte de l'audit du système d'information

Type de mesure de sécurité :

- Prévention

4.6.1.2 Analyse des risques résiduels

Le risque que nous avions décidé de laisser pour un traitement ultérieur se trouve impacté par les différentes mesures prises. Il peut donc être réévalué comme le montre le tableau 4.24. Cette réévaluation diminue la vraisemblance de survenue des scénarii et permet de rapprocher le besoin de traitement du risque de la zone « inutile de traiter ».

Risque résiduel	7. Non imputabilité des actions sur les données administratives
Gravité	Niveau 2 : la gravité est négligeable : la sécurité du dossier patient est compromise. Des données concernant un patient sont susceptibles d'être diffusées dans l'hôpital, parmi du personnel soumis au secret professionnel, mais ne prenant pas en charge ce patient
Vraisemblance	Niveau 1-2 : La menace ne se produira pas - La menace a peu de chance de se concrétiser car elle nécessite une combinaison de plusieurs facteurs sur un laps de temps prolongé

TABLE 4.24 – **Réévaluation post-mesures du risque résiduel**

4.6.1.3 Déclaration d'applicabilité

Les différents paramètres à prendre en compte, exprimés sous forme de contraintes dans la section 4.2.1.4, sont affectés par les mesures prises de la manière suivante :

1. **Contraintes légales**
   - Prises en compte : Oui.
   - Les différentes mesures proposées sont à même de mettre l'institution hospitalière en règle avec la législation actuelle. La révision régulière de ces mesures devraient également permettre de se tenir au fait des évolutions légales et éthiques.
2. **Contraintes budgétaires et conjoncturelles**
   - Prises en compte : Oui.
   - Bon nombre des mesures de sécurité proposées n'engendrent pas d'investissements conséquents qui ne seraient pas justifiés par les conséquences désastreuses que pourraient avoir les risques.
3. **Contraintes sociales**
   - Prises en compte : Non.
   - Les mesures n'ont que peu d'influence sur la manière dont l'institution appréhende son bassin de soins, par contre certaines d'entre elles devront éventuellement être accentuées en fonction de celui-ci.

4. **Contraintes temporelles sur les délais de développement et d'implémentation des logiciels**
   - Prises en compte : Non.
   - Les mesures n'ont que peu d'impacts sur les délais évoqués. L'obligation de respecter les procédures pourrait les allonger au départ, mais devrait permettre de récupérer de l'énergie à réinvestir à meilleur escient.
5. **Contraintes de personnel**
   - Prises en compte : Oui.
   - Des formations, des rappels et des actualisations régulières permettent au personnel d'appliquer les mesures de sécurité définies.
6. **Contraintes de disponibilité**
   - Prises en compte : Oui.
   - Les mesures prises doivent permettre de rester inférieur aux durées maximales définies pour les périodes d'indisponibilité. Des plans de continuité et des plans de reprise après incident sont prévus afin de maintenir une activité suffisante ou de restaurer, au mieux, la situation.
7. **Contraintes de qualité et de fiabilité des données**
   - Prises en compte : Oui.
   - Les mesures prises permettent de garantir la fiabilité et la qualité des informations recueillies au travers du dossier patient.
8. **Contraintes géographiques**
   - Prises en compte : Oui.
   - Des mesures sont prévues afin de garantir la fiabilité des informations transmises.
9. **Contraintes médiatiques**
   - Prises en compte : Oui.
   - La qualité de la gestion de l'information peut se vérifier au travers des procédures mises en place et des réponses peuvent ainsi être apportées à la demande des autorités compétentes.

4.6.2 Mettre en œuvre des mesures de sécurité

« *Cette activité fait partie du traitement des risques. Elle a pour but d'élaborer et de suivre la réalisation du plan de traitement des risques par les mesures de sécurité afin de pouvoir prononcer l'homologation de sécurité.* » [ANS10b]

4.6.2.1 Plan d'action

Dans le contexte de l'étude de la sécurité de l'information d'une institution hospitalière précise, nous aurions, à ce niveau, l'élaboration d'un plan d'application des mesures, établi sur un certain laps de temps. Dans le cadre de ce travail, nous reprendrons les différentes mesures proposées en citant les responsables de leur application, leur degré de difficulté de mise en place et l'aspect plus ou moins

prioritaire de leur exécution. Nous présenterons donc une ébauche de plan d'action (Cfr table 4.25 page 108).

Au niveau des responsabilités, nous ciblerons les grandes fonctions suivantes, déjà citées dans la section 2.2 page 12 :

- le responsable légal,
- les professionnels de la santé,
- le service « informatique »,
- les responsables de services.

En ce qui concerne l'évaluation du degré de difficulté à mettre en œuvre la mesure, nous tiendrons compte, entre autres, du niveau des compétences et de la disponibilité des ressources humaines, des moyens nécessaires en matériel, ainsi que des coûts approximatifs de déploiement (formation du personnel, investissement en matériels, recours à des firmes extérieures, ...).
Nous qualifierons ce degré de :

- élevé : le niveau de technicité exigé et les coûts à supporter s'avèrent importants,
- moyen : le niveau technique attendu correspond aux compétences des équipes en place et les coûts à supporter peuvent être intégrés dans un budget déjà établi,
- faible : la mesure peut être mise en œuvre à faible coût et nécessite des connaissances techniques de base.

La priorité sera déterminée en fonction de la gravité du risque et de la vraisemblance des scénarii que la mesure est sensée contrer. Nous optons pour un plan d'action à un an, avec des échéances intermédiaires :

- à court terme : la mesure doit être mise en œuvre aussi vite que possible,
- à moyen terme : la mesure devrait être appliquée dans un délai de 3 à 6 mois,
- à long terme : l'institution a 1 an devant elle pour réaliser un maximum des actions prévues dans le plan.

L'institution se doit, au terme de cette année, d'évaluer le travail accompli et de revoir la situation des risques afin d'actualiser le plan d'action pour la période suivante.

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
La politique de sécurité de l'information est élaborée et diffusée après validation par la direction de l'institution	Responsable légal	Faible	Court terme
Une révision de la politique de sécurité de l'information, par l'ensemble des parties prenantes, est prévue à intervalle prédéterminé, mais aussi en cas de changement de législation ou d'infrastructures	Responsable légal	Faible	Moyen terme
Il existe un soutien de la direction vis- à- vis de la sécurité de l'information, par le biais de directives, d'attribution de fonctions et de responsabilités dans la lutte contre les risques	Responsable légal	Moyen	Court terme
La coordination des mesures est assurée par les responsables nommés	Responsable de service	Moyen	Court terme
Les exigences légales et éthiques en matière de confidentialité et de secret professionnel sont clairement identifiées et actualisées	Responsable légal Professionnels de la santé Responsable de service	Faible	Court terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Les visiteurs et les sous-traitants sont systématiquement accompagnés dans les locaux sécurisés, après avoir enregistré leur présence et motif d'entrée	Tous	Faible	Court terme
Lors de la signature de contrats, les clauses de confidentialité pour les sous-traitants et les firmes de maintenance sont présentes	Tous	Faible	Court terme
Un inventaire des biens sensibles de l'institution et de leurs gestionnaires est réalisé	Responsable de service	Faible	Court terme
A chaque nouveau matériel ou technologie mis en place, une diffusion interne des règles d'utilisation est prévue	Responsable de service	Faible	Long terme
Le mode de traçabilité à mettre en œuvre pour chaque type d'information (sous-dossier) est clairement et précisément défini	Responsable légal Professionnels de la santé	Faible	Court terme
Les documents imprimés portent la marque « Confidentiel » ou « Réservé » en fonction du type de données qu'ils contiennent	Responsable de service	Moyen	Court terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Tout type de personnel signe une charte de respect de la confidentialité et une charte de responsabilisation dans l'utilisation de l'outil informatique	Responsable légal Service informatique	Moyen	Court terme
Des campagnes d'information pour sensibiliser le personnel aux risques encourus sont régulièrement organisées	Responsable légal Responsable de service	Moyen	Moyen terme
Le personnel est formé à l'usage sécurisé des applications et/ou matériels utilisés	Service informatique Responsable de service	Moyen	Long terme
Les mots de passe des firmes de maintenance sont limités à la durée minimale que leurs actions requièrent	Service informatique	Faible	Court terme
La notion de faute grave en cas d'atteinte à la confidentialité des données est inscrite dans le règlement de travail. Y figurent également les sanctions encourues	Responsable légal	Moyen	Court terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Lorsqu'un membre du personnel arrive à la fin de son contrat, ses droits d'accès (physiques et logiciels) sont immédiatement supprimés	Service informatique	Moyen	Court terme
Lors du départ d'un membre du personnel disposant du/des mots de passe « administrateur », ceux-ci sont changés	Service informatique	Moyen	Court terme
L'accès aux locaux informatiques ou recelant du matériel repris comme tel, est interdit à toute personne extérieure en-dehors de la présence d'un membre du personnel autorisé	Tous	Faible	Court terme
Des dispositifs de lutte contre l'incendie sont mis en place dans les locaux informatiques critiques (salle « machines », salle de stockage , ...)	Service informatique	Elevé	Moyen terme
Des alarmes anti-intrusions sont installées dans les locaux informatiques critiques	Service informatique	Elevé	Long terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Des consignes de fermeture à clef des locaux sont communiquées et imposées au personnel	Responsable de service	Faible	Moyen terme
Le matériel critique (serveur, équipement réseau, ...) est alimenté électriquement par plusieurs sources	Service informatique	Moyen	Moyen terme
Sur les écrans susceptibles d'être visualisés par des personnes extérieures, des films dits « de secret » sont apposés	Responsable de service	Moyen	Long terme
Une climatisation adéquate est installée dans les locaux informatiques critiques	Service informatique	Elevé	Moyen terme
Des scellés sont installés sur les ordinateurs afin de pouvoir constater leur ouverture non désirée	Service informatique	Moyen	Long terme
Des contrats de maintenance informatique sont souscrits afin de respecter les délais d'indisponibilité maximale désirée	Responsable légal Service informatique	Elevé	Moyen terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Tout équipement mis au rebut voit ses supports mémoires correctement effacés	Service informatique Responsable de service	Faible	Court terme
Il existe une documentation écrite de toutes les procédures d'exploitation existantes	Tous	Moyen	Moyen terme
Les composants inutiles des Systèmes d'exploitation sont désactivés et des procédures empêchant leurs modifications sans un accès dûment authentifié sont rédigées	Service informatique	Moyen	Moyen terme
Un système de monitoring du parc informatique est organisé	Service informatique	Elevé	Long terme
Un environnement de test permettant d'évaluer les changements logiciels ou matériels envisagés est prévu	Service informatique	Elevé	Long terme
Des rapports d'intervention sont exigés de la part des sociétés tierces intervenant sur le matériel ou les logiciels	Responsable de service	Moyen	Court terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Les ressources utilisées par les applications, les utilisateurs et les équipements sont surveillées	Service informatique	Moyen	Moyen terme
Un antivirus est installé et actualisé sur les différents Systèmes d'exploitation	Service informatique	Elevé	Court terme
Une sauvegarde « régulière » des applications et des données est réalisée, ce qui permet une récupération complète des informations	Service informatique	Moyen	Court terme
Des tests de restauration des données sauvegardées sont réalisés régulièrement afin de garantir la validité de l'ensemble de la procédure	Service informatique	Moyen	Moyen terme
Une attention particulière est apportée à la sécurisation des équipements réseaux (dans leurs accès et dans la possibilité de s'y connecter), elle est renforcée pour le matériel Wifi (non diffusion du SSID, clé WPA2, ...)	Service informatique	Elevé	Long terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Tout type de supports amovibles est rangé dans un coffre ignifuge et est détruit complètement lors de leur mise au rebut	Tous	Moyen	Court terme
La consultation de ces supports amovibles fait l'objet de procédures écrites, gardant la trace des « visiteurs »	Responsable de service	Faible	Moyen terme
Des procédures d'échange (validité, modalités, ...) et de vérification des empreintes des fichiers échangés avec les institutions extérieures sont prévues	Professionnels de la santé Service informatique Responsable de service	Elevé	Long terme
Les événements informatiques (accès, erreurs, ...) sont journalisés et analysés afin d'en corriger les causes le plus rapidement possible	Service informatique	Moyen	Court terme
Une procédure d'horodatage des actions entreprises sur les données existe	Service informatique	Moyen	Court terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Les droits d'accès des utilisateurs sont basés sur les fonctions des personnes. Ils doivent être réévalués face à tout changement applicatif ou lors de réaffectation de personnes. Ces droits font l'objet de documentations exhaustives	Service informatique	Moyen	Moyen terme
Les mots de passe font l'objet de procédures documentées quant à leur choix, de modification régulière et en tout cas à chaque suspicion de compromission	Responsable de service	Moyen	Court terme
Les équipements informatiques non utilisés bénéficient d'un verrouillage systématique, manuel et/ou automatique	Service informatique Responsable de service	Moyen	Court terme
La gestion des droits d'accès est aussi restrictive que possible en ne donnant accès qu'aux services nécessaires	Service informatique	Elevé	Court terme
La gestion du réseau permet une connexion fiable aux applications	Service informatique	Elevé	Long terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Dans la mesure du possible, l'identifiant et donc le mot de passe de l'utilisateur est géré de manière centrale (Active Directory, LDAP, ...)	Service informatique	Elevé	Long terme
Les accès nécessaires pour la maintenance des différents systèmes sont aussi courts et restrictifs que nécessaire	Service informatique Responsable de service	Moyen	Moyen terme
Les systèmes identifiés comme sensibles disposent d'un environnement spécifique	Service informatique	Elevé	Long terme
Une procédure claire est écrite pour la connexion et l'utilisation de matériel mobile (ordinateurs portables, PDA, ...)	Service informatique	Faible	Moyen terme
Une procédure claire est rédigée pour la connexion et l'utilisation du télétravail	Responsable légal	Moyen	Long terme
Suite page suivante			

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Le cahier des charges de toute nouvelle application prend en compte les exigences de sécurité et de confidentialité requises	Professionnels de la santé Service informatique Responsable de service	Moyen	Long terme
Les applications et/ou le système de base de données ont la responsabilité de vérifier la qualité des informations encodées	Professionnels de la santé Responsable de service	Moyen	Long terme
Au minimum un système RAID, ou assimilé, est mis en place sur les serveurs. La redondance du réseau et des bases de données est instaurée	Service informatique	Elevé	Moyen terme
Une politique de mesures cryptographiques (chiffrement, création d'empreintes, ...) et/ou d'anonymisation efficace est mise en place pour les envois de données à l'extérieur de l'institution hospitalière	Responsable légal Service informatique	Elevé	Moyen terme
			Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Toute modification d'applications, de matériel n'est implémentée qu'après une série de tests	Responsable de service	Elevé	Moyen terme
Tous les événements touchant la sécurité de l'information sont relatés, même et surtout s'ils sont le fait de firmes extérieures	Tous	Faible	Court terme
Toutes les traces sont conservées conformément aux dispositions légales ou éthiques	Responsable légal Service informatique	Moyen	Court terme
Des plans de secours et de reprise sont établis pour les différentes applications et matériels critiques. Ces plans doivent se coordonner entre eux, les applications et/ou matériels étant souvent « interconnectés ». Les plans sont validés et testés de manière régulière afin de s'assurer de leur justesse face aux évolutions	Professionnels de la santé Service informatique Responsable de service	Moyen	Long terme
Les assurances nécessaires (altération ou compromission des données, vol, ...) sont contractées pour le personnel et pour le matériel	Responsable légal	Elevé	Long terme

Suite page suivante

Mesures de sécurité	Responsabilité	Degré de difficulté	Priorité
Les exigences réglementaires sont être inventoriées et suivies de près	Responsable légal	Faible	Moyen terme
L'application des procédures est vérifiée par les différents responsables	Responsable légal	Faible	Court terme
Les différentes mesures de sécurité sont contrôlées de manière régulière et fixée à l'avance	Responsable légal Service informatique Responsable de service	Faible	Long terme
Les différentes traces sont particulièrement surveillées et garanties contre toute modification ou effacement	Professionnels de la santé Service informatique	Moyen	Long terme

TABLE 4.25 – **Modèle de plan d'action**

4.6.2.2 Homologation de sécurité

La mise en œuvre d'un plan de sécurité ne peut se réaliser que moyennant une implication forte des dirigeants de l'institution et une étroite collaboration avec les responsables techniques. Ceux-ci sont généralement plus à même d'être sensibilisés aux risques technologiques et à la détermination des moyens à appliquer pour y remédier.
La diffusion des informations relatives aux mesures et portant sur leurs résultats doit toujours être avalisée par les gestionnaires.
Un des moyens d'évaluer l'efficience des mesures serait de créer des tableaux de bord permettant de suivre régulièrement des indicateurs tels que : vulnérabilité, risques majeurs, incidents techniques, accidents, ...

L'homologation du plan de sécurité doit clairement être limitée dans le temps afin que celui-ci soit actualisé de manière régulière, reste pertinent et adapté aux besoins de sécurité estimés par les métiers de l'institution, et puisse prendre en compte les nouveaux risques.

Chapitre 5

Application de la méthode EBIOS au sein d'une institution hospitalière

5.1 Application pratique

Vous travaillez dans une institution hospitalière et vous vous préoccupez de la sécurité de votre dossier patient.
Comment ce travail peut-il vous aider dans votre analyse des risques ?
La méthode EBIOS procédant par itération, la première étape correspondra au contenu de ce travail moyennant que vous adaptiez les aspects généraux de façon à correspondre au cadre de votre institution.
Les 5 modules de la méthode se travaillent dans l'ordre, du premier au cinquième, mais des retours en arrière sont possibles pour vous ajuster en fonction des éléments obscurs qui apparaîtraient dans les modules suivants. Reparcourons les différents modules en mettant en évidence les points auxquels vous devez prêter attention afin de respecter le profil de votre hôpital (Cfr figure 5.1 page suivante).

Le module 1 traite de l'environnement, des mesures employées, des paramètres, des contraintes et des biens. Il peut être repris tel que proposé en veillant à ce que les évolutions légales concernant le dossier patient, qui auraient eu lieu depuis la rédaction de ce mémoire, soient prises en considération.
L'environnement décrit est général, il doit être précisé afin d'y inclure vos particularités et contraintes.
Les tableaux de mesures que nous avons présentés sont à valider par le groupe de travail que vous aurez mis en place.
De la même manière, les différents biens supports cités doivent faire l'objet d'une révision afin d'être mis en conformité avec ceux présents dans votre institution ou ceux que vous envisagez d'acquérir.

Le module 2 recherche les événements redoutés par le bien essentiel que représente votre dossier patient. Les éléments cités dans le travail sont d'application, vous devez y inclure les événements que redoutent les modifications et/ou ajouts que vous auriez introduits dans le module 1 et les classer par degré de gravité.

Le module 3 s'occupe des menaces, et de leur intrication, à l'origine des événements redoutés. Sur base des biens supports que vous avez ajoutés dans le module 1, vous devez trouver les menaces qui leur sont spécifiques et les inclure dans le tableau d'évaluation des scénarii de menaces, selon leur degré de vraisemblance.

Le module 4 met en relation les événements redoutés et les scénarri de menaces afin d'en extraire les risques. Ceux-ci seront classés en fonction des degrés de vraisemblance et de gravité afin de choisir les options de leur traitement.

Le module 5 énumère les mesures et organise leur mise en œuvre. Sur base des mesures déjà proposées dans le travail, vous devez vérifier qu'elles couvrent bien les risques que vous avez mis en évidence.
Ensuite, vous devez constituer le plan d'action à mettre en œuvre. Il sera indispensable de définir les personnes responsables des actions, de fixer un calendrier et d'envisager les freins possibles.

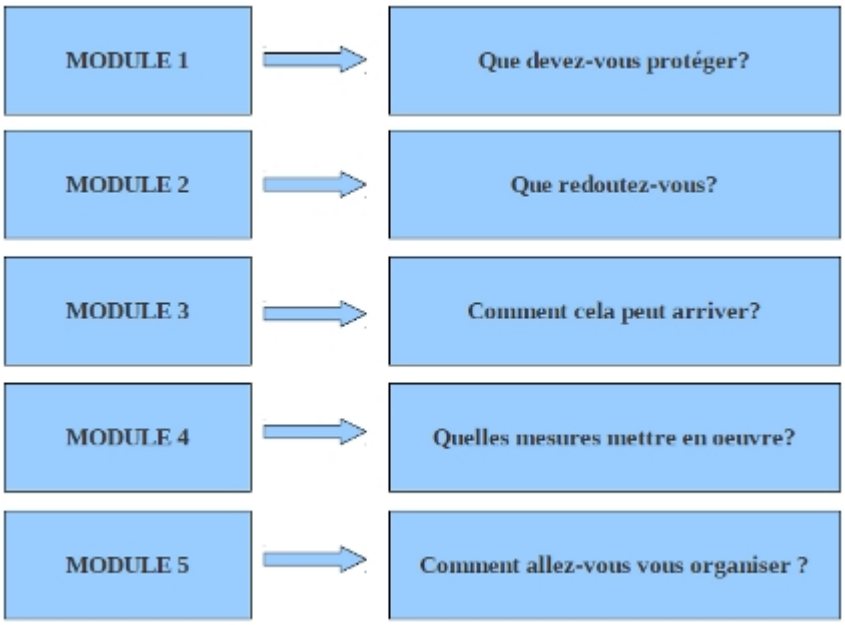


FIGURE 5.1 – **EBIOS en questions**

5.2 Mise en évidence des freins et recherche de facteurs de réussite

Nous avons choisi d'appliquer la méthode EBIOS afin de rencontrer les objectifs de sécurisation des données personnelles dans le secteur des soins de santé. Quelle que soit l'institution, l'aboutissement de la méthode prend la forme d'un plan d'action au sein duquel certains points peuvent présenter un degré de difficulté important.
Ce chapitre traitera des facteurs qui pourraient faciliter la réalisation du plan, seront abordés les aspects relatifs aux contraintes extérieures, à l'organisation, aux personnes et au budget.[Tou07]

5.2.1 En lien avec les contraintes extérieures

La sécurisation des données personnelles du dossier patient est soumise à un ensemble de contraintes légales régulièrement adaptées par le législateur. Il est donc important que l'institution organise « une veille légale ».

Les solutions logicielles, mises en place lors de l'application des mesures de sécurité, devraient intégrer protocoles standards et normalisation, afin de renforcer la qualité, la maintenance, les connaissances et la sécurité des applications déployées, sous le contrôle du personnel de l'institution hospitalière.

5.2.2 En lien avec l'organisation

La gestion d'un projet de sécurisation doit être envisagée comme l'addition de plusieurs projets, chacun d'eux étant géré par un chef de projet, prenant la responsabilité et se référant, à intervalle régulier, à un groupe de pilotage.
Le travail en « équipe projet » permettra d'être aussi exhaustif que possible, tant dans la recherche et l'analyse des risques que dans les solutions envisagées. Chaque projet sera accompagné de rapports d'avancement et d'exception.
Le groupe de pilotage doit, quant à lui et au vu de l'enjeu, comprendre au moins un membre de la Direction et des experts dans les domaines concernés.

Prenons comme exemple le modèle de plan d'action (section 4.6.2.1 page 94) : les responsabilités dans l'application de certaines mesures ont été définies comme pouvant être partagées entre plusieurs fonctions. Il est essentiel que ces différents intervenants se coordonnent afin de préciser qui fait quoi, ce qui évitera que chacun pense que c'est le rôle de l'autre.

Dans le chapitre précédent, à plusieurs reprises, nous avons mis l'accent sur la nécessité d'une communication entre les parties prenantes tout au long du processus de gestion des risques. Cette communication permet :

– de partager les informations relatives aux risques afin d'apporter l'éclairage indispensable aux orientations et décisions à prendre,
– de définir une politique cohérente au sein de l'institution,
– d'impliquer la responsabilité des décideurs dans des choix stratégiques pour l'institution,
– d'actualiser les connaissances en matière de sécurité.

5.2.3 En lien avec les personnes

Les dispositifs de sécurité ne peuvent être efficaces que s'ils sont perçus comme des bénéfices et non subis comme des contraintes. Cette perception positive de la sécurité du système d'information doit apparaître comme une des valeurs de la culture d'entreprise.

Nous insisterons sur la nécessité d'élaborer un plan de formation à la sécurité pour le personnel :
– formation de base : règles de bonne pratique, gestion des mots de passe, respect du secret médical (sur des données utiles et nécessaires, avec le consentement du patient), . . . ,
– rappel et actualisation,
– formation à la méthode choisie pour les parties prenantes,
– amélioration des compétences en lien avec les mesures du plan d'action.

La mise en place de la méthode requiert de la part des parties prenantes une grande confiance entre elles, où l'esprit d'équipe doit dominer et où la confidentialité des informations échangées est indispensable.

La mise en place d'une traçabilité des actions réalisées sur le dossier patient n'a de sens que dans la mesure où ces traces sont « surveillées » et « analysées » par les « bonnes personnes ». Certains intervenants actifs dans la sécurité [God11] estiment qu'une bonne façon de procéder est de faire gérer ces traces par l'utilisateur final lui-même.
En effet, qui d'autre, serait le plus à même de repérer une intrusion inopportune dans un dossier dont il a la charge.

5.2.4 En lien avec le budget

Par budget, nous entendons les frais liés à l'achat de matériel, au recours à des firmes extérieures, au plan de formation ainsi que les coûts salariaux des parties prenantes. Le budget engagé tiendra compte du mode de financement particulier du secteur des soins de santé, de l'histoire sociale et philosophique de l'hôpital, des choix technologiques déjà effectués et de l'orientation future envisagée.

Prenons l'exemple des mesures techniques et organisationnelles qui doivent

assurer un niveau de conservation adéquat des données. Elles seront choisies en tenant compte de l'état de la technologie actuelle, des développements futurs, des frais qu'entraîne leur application, de la nature des données à protéger et des risques potentiels. [Ell03] Il faut toujours mettre en adéquation le risque et le coût de son traitement. [DN06]
Il serait aberrant que les coûts de mise en œuvre des mesures soient plus élevés que ceux entrainés par les risques encourus. Une réduction de ces coûts peut s'envisager, dans la méthode EBIOS, grâce à l'utilisation de modèles génériques et à une application progressive et cyclique de l'étude.

Face à des coûts qui peuvent être importants, une institution aura toujours tendance à les inscrire au budget de l'année suivante. Le report dans la prise de certaines mesures n'est pourtant pas envisageable.

Conclusion

La sécurisation des données d'un dossier de soins informatisé est indispensable à la garantie d'une continuité dans la prise en charge du patient. Elle est sous la responsabilité légale et finale du gestionnaire de l'institution hospitalière, mais implique l'ensemble des acteurs internes, voire externes au milieu.

Intégrer les principes de sécurisation des données dans la pratique journalière des professionnels de santé, et dans leur culture, reste une gageure. Ceux-ci ont bien souvent tendance à ne voir dans l'informatisation qu'une simple transposition des supports papier qu'ils connaissaient tout en admettant que les possibilités d'accès aux données s'en trouvent élargies. Inhérent à un accès aisé, des brèches dans la sécurisation pourraient s'avérer plus nombreuses, d'où la nécessité de mettre en place des mesures de prévention et d'impliquer de manière active les différents acteurs. Convaincre les professionnels de santé de l'importance d'agir pour la sécurité des données du dossier patient reste une entreprise de longue haleine, leur préoccupation première étant les soins aux patients.

Compte tenu des exigences légales et éthiques, et afin de déterminer les mesures pertinentes répondant aux besoins d'une institution hospitalière, nous avons, de manière théorique, analysé l'environnement et élaboré un plan d'action selon la méthode EBIOS. Les étapes de la méthode sont la description du contexte hospitalier, l'étude des événements redoutés, l'identification des scénarri de menaces, l'évaluation des risques et le choix des mesures à apporter.

La diffusion de l'information liée à la gestion des risques permet de construire l'espace de confiance nécessaire au déploiement réussi d'un informatisation complète du dossier patient au sein de l'institution hospitalière.
Espace de confiance comprenant la confiance dans l'identité et la qualification des personnes prenant en charge un dossier, dans l'intégrité des informations que le dossier contient et finalement dans la réaction aux « attaques » dont le système d'information pourrait faire l'objet.
La mise en route d'un processus d'amélioration du niveau de sécurité par une meilleure gestion des risques au travers de mesures cohérentes et reconnues dans un référentiel international permettrait d'évoluer, si le législateur nous y poussait, vers une certification.

Au terme de ce travail, nous sommes parvenus à élaborer un modèle de plan d'action permettant de sécuriser les données contenues dans le dossier de soins d'un patient.
Le choix de la méthode EBIOS s'est avéré adapté à l'objectif de ce travail. Appliquée à une institution déterminée, nous pensons que le caractère progressif et itératif de la méthode constitue un atout.
En effet, elle permet de prendre contact avec la gestion des risques en commençant par le relevé des éléments constitutifs de l'environnement intra et extra hospitalier. Elle se poursuit de façon logique en suivant les différents modules, l'itération permet de préciser chacune des étapes et ainsi assurer au processus une progression constante.

La sécurisation de ces données est un des grands enjeux de l'informatisation croissante que connaît le monde hospitalier. Enjeu pour répondre aux exigences légales, mais aussi aux attentes des utilisateurs ou encore à celles des patients eux-mêmes.

Ces derniers seront amenés, dans les prochaines années, à intervenir de manière encore plus prononcée dans la gestion des données les concernant.
Une grande question reste donc ouverte après cette analyse de risque : quelle est l'implication du patient dans la gestion de son dossier ?
Toute la partie touchant aux droits du patient n'ayant été qu'effleurée, la gestion de ce type d'accès, constitue un objectif de continuité de ce travail.

Bibliographie

[27005a] ISO/IEC 27001. *Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences.* International standard, 2005.

[27005b] ISO/IEC 27002. *Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information.* International standard, 2005.

[27005c] ISO/IEC 27005. *Technologies de l'information - Techniques de sécurité - Gestion du risque en sécurité de l'information.* International standard, 2005.

[ANS10a] ANSSI. *EBIOS : la méthode de gestion des risques SSI. Un outil simple et puissant.* Agence nationale de la sécurité des systèmes d'information, Paris, Avril 2010.

[ANS10b] ANSSI. *Expression des Besoins et Identification des Objectifs de Sécurité.* Agence nationale de la sécurité des systèmes d information, Paris, Janvier 2010.

[ANS10c] ANSSI. *Référentiel Général de Sécurité.* Agence nationale de la sécurité des systèmes d'information, Paris, Mai 2010.

[Bel87] Etat Belge. Loi sur les hôpitaux, coordonnée le 7 août 1987. *Moniteur Belge, 07 octobre 1987*, 1987.

[Bel92] Etat Belge. Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. *Moniteur Belge, 18 mars 1993*, 1992.

[Bel99] Etat Belge. Arrêté royal déterminant les conditions générales minimales auxquelles le dossier médical doit répondre. *Moniteur Belge, 30 juillet 1999*, 1999.

[Bel02] Etat Belge. Loi relative aux droits du patient. *Moniteur Belge, 26 septembre 2002*, 2002.

[Bel06] Etat Belge. Arrêté royal déterminant les conditions générales minimales auxquelles le dossier infirmier, visé à l'article 17quater de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre. *Moniteur Belge, 30 janvier 2007*, 2006.

[DN06] H. De Neve. La dualité de l'informatisation dans les hôpitaux. *Hospitals.be*, 4(4) :5, 2006.

[Ell03] E. Ellenberg. Le management des risques à l'hôpital. *Revue ADSP du Haut Conseil de la Santé Publique*, (45) :63–66, 2003.

[God11] Frans Godden. Table ronde : La sécurité IT ne peut être un phénomène isolé. *Datenews numéro 7 15 avril 2011*, 2011.

[GVT01] P. Gilbert, J.C. Vandecasteele, and L. Treccani. La politique globale de gestion du risque au CHU de charleroi. *Hospitals.be*, 4(247), 2001.

[Her09] Jean Herveg. *La protection des données du patient dans l'hôpital*. Kluwer, 2009.

[Hub10] Jean-Marie Hubaux. Les dix commandements du juriste face aux TIC. In *Les technologies de l'information et de la communication : amies ou ennemies*, La Marlagne, Décembre 2010. Groupement Hospitalier Namurois.

[PVE10] Patrick Prof Van Eecke. Privacy 101 : a beginner's guide to data protection. In *An introduction to the Data Protection Directive*, Bruxelles, November 2010. Privacy and scientific Research : from Obstruction to Construction.

[San09] ASIP Santé. Cahier des clauses techniques particulières. DMP1 - hébergement, Agence des systèmes d'information partagés de Santé, Paris, Octobre 2009.

[Tou07] Philippe Tourron. Expression des besoins et identification des objectifs de sécurité. In *Présentation projets EBIOS*. EBIOS Université de la méditerranée, Octobre 2007.

[VB03] A. Vandenberghe and M. Bangels. Le dossier médical sur l'internet. *Hospitals.be*, 4(2), 2003.