

**Déclinaison du Référentiel Général d'Interopérabilité
et
Démarche d'élaboration des Référentiels de Santé**

**Fiche de synthèse du thème n°5
Sécurité**

Version 1.0

Sommaire

1.	Présentation du thème.....	5
1.	Présentation du thème.....	5
1.1	Situation du thème.....	5
1.2	Définitions.....	5
1.2.1	Critères de sécurité.....	5
1.2.2	Fonctions de sécurité.....	5
1.3	Objectifs et enjeux.....	6
1.3.1	Objectifs.....	6
1.3.2	Enjeux.....	6
1.3.3	Contraintes.....	8
1.4	Présentation du document.....	8
2.	Etat de l'art.....	9
2.1	Etat des normes internationales.....	9
2.1.1	Normes internationales touchant à la gouvernance sécurité.....	9
2.1.2	Normes techniques.....	11
2.1.3	Référentiels de sécurité.....	12
2.1.4	Référentiels spécifiques au monde de la santé.....	13
2.2	Gouvernance sécurité.....	13
2.3	Elements de sécurité technique.....	15
2.3.1	Fonctions de sécurité.....	15
2.3.2	Bonnes pratiques de la sécurité.....	16
2.3.3	Synthèse.....	17
3.	Cadre réglementaire.....	18
3.1	Réglementation et codes.....	18
3.2	Lois informatique et libertés.....	18
3.3	Lois générales sur la sécurité de l'information.....	19
3.3.1	Lois sur la signature électronique et l'usage de la cryptographie.....	19
3.3.2	Loi sur l'archivage légal.....	19
3.3.3	Certification des produits de sécurité.....	19
3.3.4	Lutte contre la fraude informatique.....	19

3.4	LOIS SPECIFIQUES AU MILIEU DE LA SANTE	20
4.	Recommandations du RG*	21
4.1	RGI : Recommandations / Règles	21
4.2	RGS : Recommandations / Règles	24
4.3	Commentaire	27
5.	Recomandations appliquées à la santé	28
5.1	Recommandations GMSIH	28
5.2	recommandations HL7	28
5.3	Modèle OrBAC	28
5.4	recommandations IHE	29
5.5	Référentiels techniques spécifiques	29
5.5.1	Homologation OSM	29
5.5.2	Sécurisation DICOM	30
6.	Conclusions	31
1.2	Définitions	5
1.2.1	Critères de sécurité	5
1.2.2	Fonctions de sécurité	5
1.3	Objectifs et enjeux	6
1.3.1	Objectifs	6
1.3.2	Enjeux	6
1.3.3	Contraintes	8
1.4	Présentation du document	8
2.	Etat de l'art	9
2.1	Etat des normes internationales	9
2.1.1	Normes internationales touchant à la gouvernance sécurité	9
2.1.2	Normes techniques	11
2.1.3	Référentiels de sécurité	12
2.1.4	Référentiels spécifiques au monde de la santé	13
2.2	Gouvernance sécurité	13
2.3	Elements de sécurité technique	15
2.3.1	Fonctions de sécurité	15
2.3.2	Bonnes pratiques de la sécurité	16
2.3.3	Synthèse	17
3.	Cadre réglementaire	18
3.1	Réglementation et codes	18
3.2	Lois informatique et libertés	18
3.3	Lois générales sur la sécurité de l'information	19
3.3.1	Lois sur la signature électronique et l'usage de la cryptographie	19
3.3.2	Loi sur l'archivage légal	19
3.3.3	Certification des produits de sécurité	19

3.3.4	Lutte contre la fraude informatique	19
4.	Recommandations du RG*	21
4.1	RGI : Recommandations / Règles	21
4.2	RGS : Recommandations / Règles	24
4.3	Commentaire	27
5.	Recommandations appliquées à la santé	28
5.1	Recommandations GMSIH	28
5.2	recommandations HL7	28
5.3	Modèle OrBAC.....	28
5.4	recommandations IHE	29
5.5	Référentiels techniques spécifiques.....	29
5.5.1	Homologation OSM	29
5.5.2	Sécurisation DICOM	30
6.	Conclusions	31

1. PRESENTATION DU THEME

1.1 SITUATION DU THEME

Dans le cadre de l'étude « Déclinaison du RGI démarche d'élaboration des référentiels de santé », des thèmes de travail ont été déterminés afin de rapprocher les spécificités propres du domaine de la santé aux référentiels généraux produits par la DGME. Neuf thèmes ont ainsi été retenus. Ces thèmes sont les suivants :

1. Démarche et concepts ;
2. Modèles conceptuels de santé ;
3. Accès aux annuaires et répertoires ;
4. Utilisation de règles dans les systèmes d'information ;
5. Sécurité ;
6. Dématérialisation des échanges (en particulier avec AMO/AMC, format de données et de documents) ;
7. Information et services utiles aux citoyens, usagers et patients ;
8. Traçabilité (historique médical, décision médicale, information médicale);
9. Gestion des configurations – Architecture de communication.

Chaque thème fait l'objet d'une analyse dans le cadre de groupe de travail et la synthèse des travaux fait l'objet d'une fiche.

Ce document constitue la fiche du cinquième thème « Sécurité ».

1.2 DEFINITIONS

1.2.1 Critères de sécurité

- **Disponibilité** : faire en sorte que les utilisateurs autorisés puissent accéder à l'information et aux biens auxquels elle est associée, lorsqu'ils en ont besoin.
- **Intégrité** : protéger l'exactitude et l'intégrité de l'information et des méthodes de traitement.
- **Confidentialité** : faire en sorte que l'information ne soit accessible qu'aux personnes autorisées à y accéder
- **Preuve** : Les moyens de preuve et contrôle nécessaires aux utilisateurs pour accorder leur confiance dans l'information fournie

1.2.2 Fonctions de sécurité

- **Identification** : Associer à tout individu identifiable et au moyen d'un système d'étiquetage, au sens « nommage », un (au moins) identifiant permettant de discerner/discriminer cet individu parmi l'ensemble d'une population concernée d'individus répertoriés.
- **Authentification** : Confirmation de l'identité de l'entité déclarée. L'authentification correspond à l'action de vérifier une identité déclarée de manière à contribuer à l'authenticité d'actions à venir ou documents, ressources destinées à être traitées.

- **Habilitation** : Droit accordé à un individu d'accéder à des informations dont le niveau de sécurité est inférieur ou égal à un niveau déterminé.
- **Chiffrement**: Processus cryptographique permettant de transformer des données en clair en données illisibles par des personnes non autorisées.
- **Signature** : Moyen cryptographique apportant la preuve de l'intégrité d'un message, validé par une personne signataire.
- **Non-répudiation** : Apporte la preuve de l'origine ou de la livraison des données afin de protéger l'émetteur contre une fausse déclaration de non réception par le destinataire et le destinataire contre une fausse déclaration de non-émission par l'émetteur. Généralement établi par un tiers de confiance.
- **Profil d'accès utilisateur** Pour chaque utilisateur individuel, ou chaque groupe particulier d'utilisateurs, regroupés par exemple par projet, on établit un "profil", comportant :
 - Une identification (nom, fonction, organisation, etc.),
 - Une matrice d'accès et habilitation propre à cet utilisateur ; en fonction du type et de la classe de données
- **Anonymisation** : quelle que soit sa forme technique : organisationnelle, manuelle, électronique, cryptographique, permet d'éliminer toute relation directe ou indirecte entre, un ou plusieurs éléments d'information à caractère personnel, et la personne physique à laquelle ils correspondent.
- **Pseudonymisation** : Action de transformation de l'identité de la personne en un élément identifiable permettant de conserver la cohérence de l'ensemble des données tout en protégeant l'identité de la personne.

1.3 OBJECTIFS ET ENJEUX

1.3.1 Objectifs

Ce thème présente les différentes approches, normes et standards de sécurité s'appliquant au monde de la santé. Il rappelle les principes de sécurité majeurs et leur application possible aux professionnels de santé.

Cette analyse s'appuie sur les concepts classiques de sécurité et notamment ceux définis dans les normes internationales comme les bonnes pratiques de l'ISO 27002, le Système de Management de la Sécurité de l'Information (SMSI) ISO 27001 et sa déclinaison au monde de la santé ISO 27999. Elle s'appuie de même sur les préconisations des référentiels RG* et notamment le RGS et le RGI ainsi que sur les référentiels émis par des organisations du milieu professionnel de santé comme l'IHE, le HL7 ou encore les précédents travaux du GMSIH.

Le présent document n'a pas pour ambition de réaliser une comparaison exhaustive des normes de la santé avec le RGI ou le RGS. Les rapprochements qui y sont faits sont donnés pour illustrer une démarche qui est en cours de construction (outil de comparaison des référentiels).

1.3.2 Enjeux

Les principaux enjeux de la sécurité dans le milieu de la santé visent principalement à mettre en place les moyens nécessaires destinés à :

- Assurer la fourniture des services de santé ;

La mission principale du monde professionnel de la santé est de s'assurer que les services aux patients sont réalisés dans de manière efficace et juste. Le soin accordé au patient et sa qualité est la principale priorité à considérer. L'évolution du monde de la santé ainsi que la modernisation des établissements de santé conduiront de plus en plus vers une dématérialisation des échanges et des informations médicales. Les soins et la qualité de la prestation médicale reposant de plus en plus sur la qualité de l'information, il faut que le Système d'Information puisse répondre à un niveau d'exigence fort en terme de sécurité en matière de disponibilité et d'intégrité.

- Protéger les données personnelles du patient ;

Les données médicales du patient comprenant notamment le dossier médical personnel, sont protégées par la déontologie médicale, et le cadre légal défini notamment par les lois informatique et libertés. Cette protection doit donc restreindre les accès à ces données au personnel médical ayant besoin d'y accéder lors de la prise en charge du patient, avec son consentement, et l'anonymisation des données lors de traitements statistiques.

- Protéger les biens de la recherche ;

La recherche médicale pour celui qui la pratique constitue à la fois un avantage économique du laboratoire, ainsi qu'un enjeu pour la santé en général. Les données recueillies pour la recherche médicale, et qui sont informatisés, doivent être protégées principalement en intégrité et confidentialité.

- Eviter les erreurs de prescription ;

Les prescriptions sont généralement réalisées de manière informatisée. La prescription elle-même peut être transmise de manière informatique, ou être générée à partir d'un logiciel d'aide à la prescription. La protection de l'intégrité de la prescription et le contrôle de la cohérence de la prescription, doit permettre d'éviter des erreurs au niveau des soins fournis au patient.

- Assurer la protection contre l'utilisation non autorisée des services de santé et prévenir la fraude ;

Il peut être aisé d'obtenir un accès non autorisé à une application de santé (par exemple via l'accès à un poste de travail non verrouillé). Les utilisateurs autorisés peuvent de même effectuer des actions non autorisées, comme l'altération malicieuse des données.

- Assurer la bonne identification du patient ;

Effectuer une identification correcte du patient au niveau informatique et pouvoir lier son identité à son historique médical, est crucial. D'autre part, les cas d'usurpation d'identité sont à considérer, les informations médicales et l'identité médicale d'un patient pouvant servir de base à une usurpation d'identité dans d'autres systèmes de l'administration.

- S'assurer du consentement du patient pour les traitements informatiques et les soins.

Le consentement aux soins, nécessitant une information précise de la part des équipes soignantes et médicales, est une exigence des personnes malades. De nombreux textes précisent déjà le droit à l'information et le principe du consentement libre et éclairé.

La prise en compte de l'ensemble de ces enjeux permet :

- d'assurer un niveau de confiance des usagers vis-à-vis du système d'information en place et le système de soin,
- d'apporter un niveau d'engagement de responsabilité des professionnels de santé.

1.3.3 Contraintes

Les projets d'amélioration de la sécurité doivent prendre en compte la problématique d'applicabilité de mesures, ou des obligations de sécurité, dans les différents environnements relatifs au milieu de la santé. Les contraintes opérationnelles locales à chaque établissement et les contraintes propres au métier de la santé doivent être pris en compte dans la démarche de sécurité.

Il faut ainsi pouvoir prendre en compte les différents aspects liés aux :

- Moyens propres de chaque établissement ;
- Contraintes de performance et de temps de réponses, pouvant être critiques en cas d'urgences ;
- Contraintes de déploiement et de gestion de la configuration notamment dans les cabinets de médecine de ville.

1.4 PRESENTATION DU DOCUMENT

Ce document constitue la fiche de synthèse du thème « Sécurité ». Il est destiné aux établissements de santé et aux réseaux de santé pour les guider dans leurs choix de standards et d'interopérabilité.

Le document amorce une comparaison entre les préconisations des RG* et les standards et normes utilisés dans la santé.

2. ETAT DE L'ART

La sécurité de l'information est un élément majeur permettant de garantir un niveau de confiance dans l'infrastructure informatique et les services informatiques fournis aux utilisateurs. Cette sécurité vise à atteindre les objectifs de sécurité définis en matière de disponibilité, intégrité, confidentialité, preuve et contrôle, et apporter un niveau de protection des biens informationnels suffisant par rapport aux risques liés à l'activité médicale

La sécurité peut s'envisager sous deux aspects :

- L'angle gouvernance, qui va traduire la mise en place d'une organisation dédiée à la gestion de la sécurité, et son amélioration constante ;
- L'angle technique, qui va décrire l'ensemble des mesures techniques de sécurité à mettre en place dans un mode projet.

En France, les initiatives concrètes en sécurité informatique sont poussées par :

- Les lois et les décrets touchant à la sécurité informatique et la protection des données personnelles ;
- Les clubs de réflexion comme le CLUSIF ;
- La DCSSI qui propose un certain des guides et référentiels de sécurité, et qualifie les outils de sécurité.

Dans le milieu de la santé, la réglementation, et notamment le décret confidentialité du 15 mai 2007 impose à l'établissement de santé de respecter un certain nombre de règles en terme de sécurité comme la protection des données du patient (le DMP), l'utilisation de la carte CPS... L'existant en matière de sécurité appliquée aux établissements de santé et réseaux de santé, provient de plusieurs sources :

- Les études du GMSIH ;
- Les préconisations des organisations internationales comme l'IHE, le HL7;
- Les implémentations techniques dans les outils existants.

Les prochains chapitres dressent un panorama général de l'état de l'art en terme de sécurité informatique sans entrer dans les spécificités et donnent des exemples propres au monde de la santé qui seront décrit au paragraphe 5.

2.1 ETAT DES NORMES INTERNATIONNALES

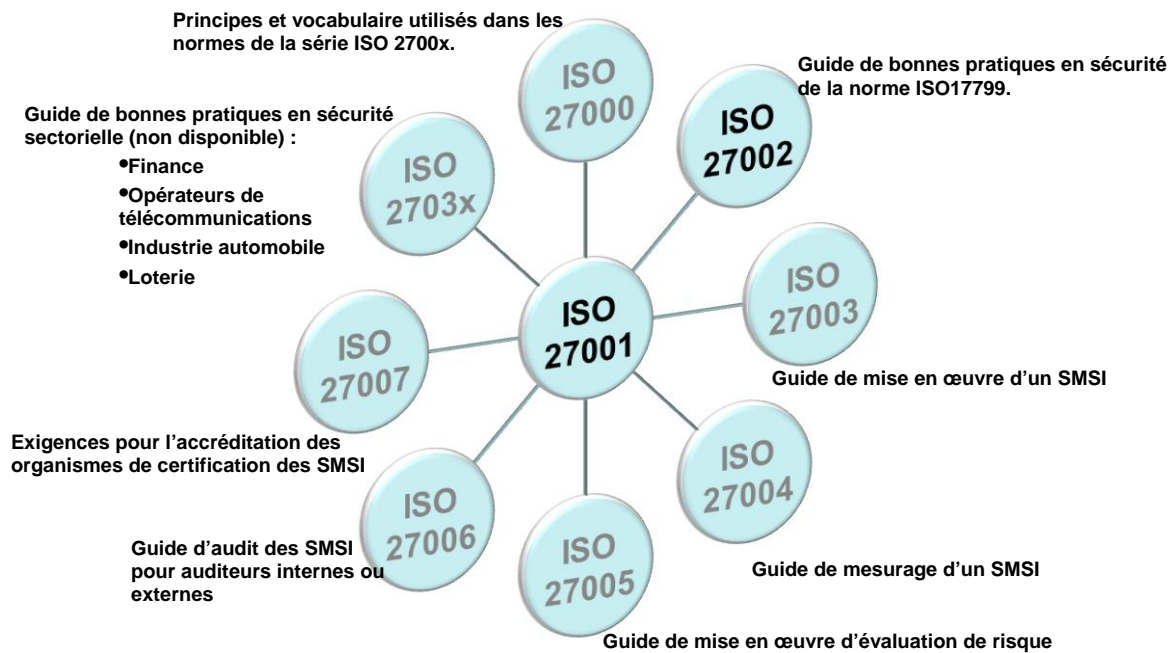
2.1.1 Normes internationales touchant à la gouvernance sécurité

Les principales normes sur les Systèmes de Management concernant l'information sont les suivantes:

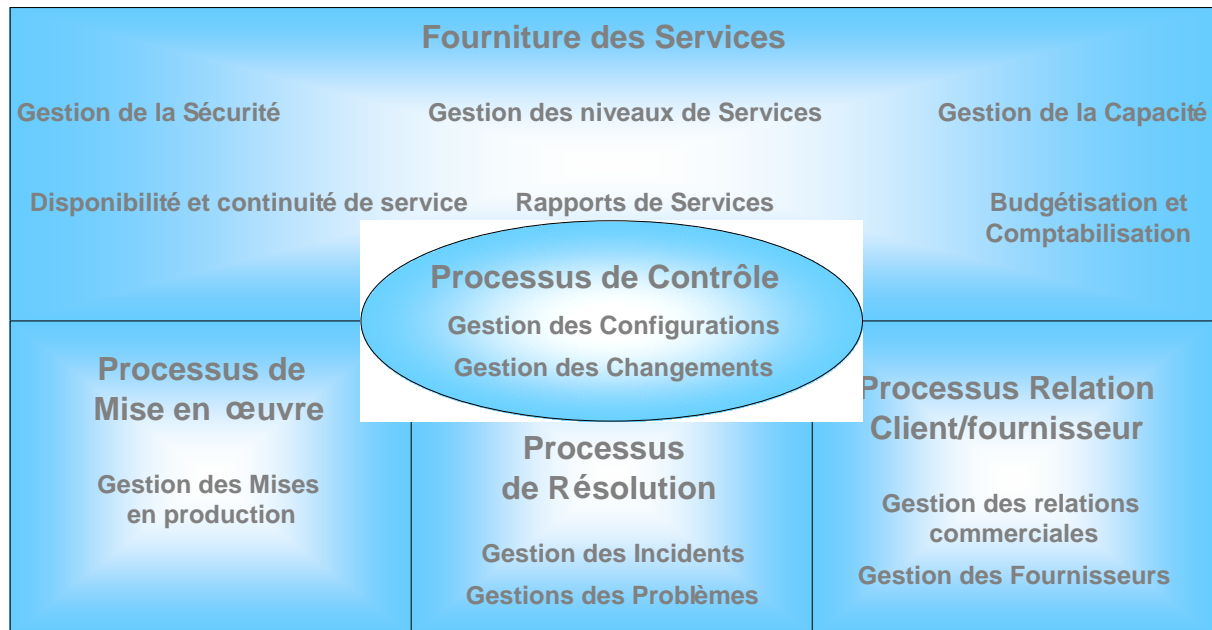
- **ISO 27001:2005**: décrivant les principes et étapes de mises en œuvre d'un SMSI (Système de Management de la Sécurité de l'Information) en proposant le passage d'une approche réactive de la sécurité à une approche proactive par la mise en place de processus.
- **ISO 27799:2006**: constituant l'adaptation de l'ISO 27001:2005 et de l'ISO 27002 :2005 au monde de la santé, dont voici le plan :
 - **1: Scope**
 - **2: References**
 - **3: Terminology**

- 4: Symbols
- 5: Health information security
- 6: Practical Action Plan for Implementing ISO 17799/27002
- 7: Healthcare Implications if ISO 17799/27002
- 8: Annex A: Threats
- 9: Annex B: Tasks and documentation of the ISMS
- 10: Annex C: Potential benefits and tool attributes
- 11: Annex D: Related standards

L'ensemble des normes ISO 2700X autour de la gestion de la sécurité de l'information peut être représenté par le panorama suivant :



- **ISO 20000** : La norme ISO/CEI 20000 encourage l'adoption d'une approche par processus pour fournir efficacement les services informatiques destinés à répondre aux exigences du business et des clients. L'ISO 20000 reprends les concepts du référentiel ITIL, en présentant un ensemble restreint de processus. Les processus détaillés dans la norme ISO 20000 sont les suivants :



D'autre part, la communauté européenne a diffusé un certain nombre de normes autour de la sécurité informatique, au travers de deux comités :

- Le CEN/TC 251 : Comité technique sur l'informatique de santé, évoquant entre autres les aspects sécurité
- Le CEN/TC 224 : Comité autour de la signature électronique et la carte ECC

2.1.2 Normes techniques

- **ISO 18028** : Suite de cinq normes (ISO 18028-1 à ISO 18028-5) définissant un cadre général pour mettre en place et maintenir un niveau de sécurité technique au niveau des réseaux de communication.
- **ISO 15408:2005** : Définit les critères d'évaluation des produits en termes de sécurité et les processus d'évaluation et de délivrance de niveau de confiance.
- **ISO 18043:2006** : Définissant l'ensemble des critères de choix et de mise en place de systèmes de détection d'intrusion.
- **ISO 7816** : Normes définissant les règles de gestion de cartes à puces électroniques.

- **ISO 17090 :**

Suite de trois normes définissant, le cadre de la PKI, des profils de certificat, et définissant la gestion des politiques d'autorité de certification.

- **Standards WS-Security :**

Standards industriels issus du groupement OASIS, définissant les critères techniques d'implémentation de services de sécurité dans une architecture Web Service.

2.1.3 Référentiels de sécurité

- **COBIT, CMMI, ITIL**

- COBIT, est un référentiel de mesure et de bonnes pratiques en matière de gouvernance IT. Il constitue un framework pour la gestion IT, et la gestion des risques.

- CMMI pour Capability Maturity Model Integration présente dans une approche par processus, les éléments nécessaires à l'évaluation de niveaux de maturité dans l'organisation et la gestion IT.

- ITIL est un référentiel de bonne pratique traitant de la mise en place d'une gouvernance IT basée sur les principes globaux de gestion du changement, de la configuration, des incidents et des problèmes, de la continuité de service, des mises en productions de la gestion financières et de la sécurité.

- **Analyse de risque (EBIOS, MEHARI, ...)**

L'analyse de risque est la base des travaux de sécurité. Elle permet d'identifier les risques encourus par un système, de définir les objectifs de sécurité que le système vise, et de traiter les risques résiduels.

Il existe de nombreuses méthodes d'analyse de risques, nous pouvons citer : EBIOS issu de la DCSSI, MEHARI issu des travaux du CLUSIF, CRAMM (**CCTA Risk Analysis and Management Method**) a été conçue en 1986 par le CCTA sous l'impulsion du gouvernement britannique, OCTAVE créée par l'Université de Carnegie Mellon, sur la base de travaux du CERT, en 1999.

- **Critères communs et qualification DCSSI**

La certification selon les critères communs suit le standard ISO 15408 et s'inscrit dans un schéma de reconnaissance internationale. En France, l'organisation en charge de la certification critères communs, en partenariat avec les CESTI (Centres d'Evaluation de la Sécurité des Technologies de l'information), est la DCSSI. Les niveaux d'exigences critères communs permettent de garantir que le produit de sécurité remplit bien des critères de pérennité, ainsi que de sécurité dans son développement et sa réalisation.

- **RG* : référentiels généraux de la DGME**

Le RGI et le RGS sont des référentiels issus de la DGME, définissent des règles de sécurité et d'interopérabilité à mettre en place dans l'administration française. Le RGI présente un certain nombre de choix techniques de sécurité autour d'éléments permettant d'interopérer les systèmes de sécurité. Le RGS présente à la fois une vision gouvernance de la sécurité ainsi qu'une vision axée fonctions de sécurité.

- **PRIS v2.1**

La PRIS ou Politique de Référencement Intersectoriel de Sécurité, constitue un ensemble de documents issus de travaux du MINEFI, définissant un ensemble de règles autour de services de cryptographie à clef publique.

2.1.4 Référentiels spécifiques au monde de la santé

Les référentiels suivants sont des éléments issus directement de travaux destinés à interopérer et sécuriser les outils informatiques propres à la santé.

- **Critères d'homologation OSM et sécurisation des messages**

Le GIP CPS fournit un référentiel destiné à assister les industriels à développer une solution de sécurisation des messageries utilisées par les porteurs de carte CPS. A ce titre, le référentiel constitue une base sur laquelle le produit de sécurisation pourra-t-être homologué. Ce document présente des exigences de sécurité principalement autour du profil cryptographique devant être utilisé par les outils candidats à l'homologation.

- **Sécurisations des échanges DICOM**

La sécurisation d'imagerie médicale DICOM est basée sur l'utilisation de chiffrement et la pseudonymisation des échanges DICOM.

- **Recommandations issues d'organismes :**

- IHE
- HL7 et HPRIM
- GMISH (travaux effectués en 2003)

Ces éléments seront détaillés au paragraphe 4.

- **Norme FD S 97 – 560 :**

La norme FD S 97 – 560 présente des critères et moyens permettant de s'assurer de l'anonymisation de données à caractères personnels.

- **Règles et standards américains autour de la santé:**

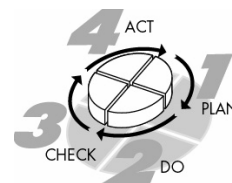
- Règles et standards du HIPAA autour de la confidentialité de l'information
- FDA régulation 21 CFR Part 11

Les éléments spécifiques au milieu de la santé sont détaillés au chapitre 5.

2.2 GOVERNANCE SECURITE

Le système de management de la sécurité de l'information, que l'on peut définir comme composé des activités coordonnées permettant d'orienter et de contrôler un organisation en matière de sécurité de l'information, est basé sur une approche de la gestion du risque, décrite principalement au sein de la norme ISO 27001. Il s'appuie sur le principe que toutes les informations et tous les systèmes qui les traitent :

- N'ont pas la même valeur ;
- Ne sont pas soumis aux mêmes menaces ;
- N'ont pas les mêmes vulnérabilités.



Le Système de Management de la Sécurité de l'Information (SMSI) est un processus faisant partie intégrante de l'organisation. Cette notion de système de management est à rapprocher des notions de système qualité introduites par l'ISO9000 et l'ISO14000. Le SMSI est basé sur une approche de gestion des risques visant à définir, mettre en œuvre et continuellement vérifier / maintenir / améliorer la sécurité de l'information, à partir d'un ensemble d'éléments corrélés ou interactifs. Il est nécessaire de formaliser la mise en œuvre de cette approche de management de la sécurité de l'information en appliquant le principe de la roue de Deming selon les phases suivantes :

Planifier (Plan)

- Définir les objectifs, la stratégie, la politique globale de sécurité ;
- Définir l'organisation de la sécurité de l'information ;

- Analyser les risques ;
- Définir un plan de traitement des risques (ou plan de sécurité).

Faire – Implémenter (Do)

- Mettre en œuvre les mesures de protection ;
- Assurer la sensibilisation et la formation des personnels ;
- Approuver (homologation, agrément) les Systèmes d'Information.

Vérifier – Contrôler (Check)

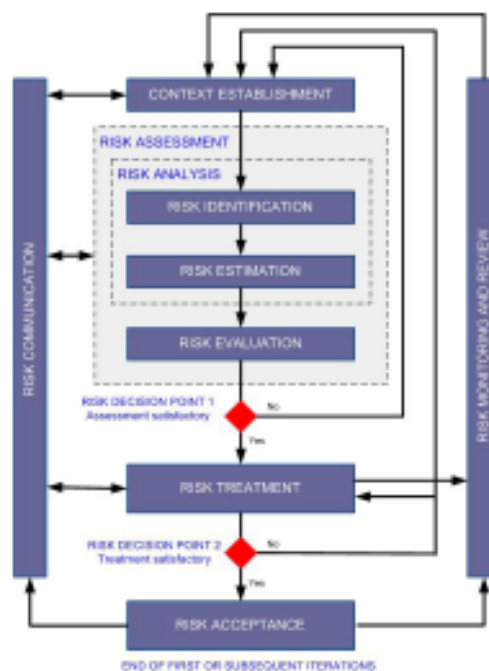
- Vérifier régulièrement la conformité des mesures de protection avec le plan de sécurité ;
- Revoir régulièrement les niveaux de risques résiduels et acceptés en fonction des évolutions de l'organisation, des systèmes et technologies mis en œuvre, des menaces, etc. ;
- Mettre en œuvre des procédures de gestion des configurations et du changement ;
- Mettre en œuvre un schéma de gestion des incidents de sécurité.

Réagir (Act)

- Assurer l'administration et la maintenance (préventive / corrective) des mesures de protection mises en œuvre ;
- Identifier et implémenter les évolutions requises sur les différentes mesures de protection.

Dans ce contexte, l'analyse et le traitement des risques constituent un des fondements d'une bonne gestion de la sécurité au sein d'une entreprise. Au sein d'un projet, l'analyse de risque permet de définir les mesures de protection adéquates aux besoins de sécurité du projet, et d'assurer un niveau de confiance validé et homologué dans le service informatique fourni.

Le diagramme ci-dessous présente les principales étapes d'une analyse de risque tel que défini au niveau de la norme ISO 27005



- **Identification du risque**
 - Identification des actifs et des menaces, vulnérabilités
 - Identification des conséquences (en terme DICP ou IFOJ*)
 - Évaluation des mesures actuelles
- **Estimation du risque**
 - Estimation qualitative et/ou quantitative
 - Évaluation des conséquences (ex :DICP ou IFOJ)

- Probabilité de la menace
- Évaluation des vulnérabilités
- Estimation du niveau de risque
- **Appréciation du risque**
 - Consolidation
 - Classement par ordre de priorité les risques
 - Importance du processus métier ou des actifs concernés
- **Traitement du risque**
 - Décision : Acceptation, Transfert, Suppression, Réduction
 - Responsable

* : DICP : Disponibilité, Intégrité, Confidentialité, Preuve. IFOJ : Interne, Financier, Organisationnel, Juridique.

2.3 ELEMENTS DE SECURITE TECHNIQUE

2.3.1 Fonctions de sécurité

Suite à l'expression des besoins de sécurité, il convient de considérer les mesures de protection à mettre en place pour atteindre la cible de sécurité. Les fonctions de sécurité permettent d'ajouter des niveaux de protection permettant d'augmenter ce niveau de sécurité.

Les principales fonctions de sécurité sont les suivantes :

- **Gestion de la cryptographie :**
 - Chiffrement et signature :
 - Utilisation de standards algorithmiques comme AES, 3DES, RSA, DSA, XAdES,...
 - Possibilité d'utiliser la carte à puce CPS pour effectuer la signature.
 - Règles concernant les outils cryptographiques :
 - Certification critères communs par la DCSSI
 - Gestion des clefs cryptographiques (se basant sur les travaux de la PRIS) :
 - Mise en place de politiques de certificat ;
 - Mise en place de politiques de signature, d'horodatage ;
 - Gestion des gabarits de certificats.

- **Sécurisation des flux :**

Cette fonction consiste à protéger les flux d'échange de donnée via l'utilisation de protocoles de chiffrement spécifique, parmi lesquels on peut citer :

- TLS 1.1, SSL v3.0,... pour le chiffrement et l'authentification client / serveur ;
- Diffie Hellman pour l'échange de clefs ;
- NTP pour la synchronisation temporelle.

- **Identification, authentification**

Cette fonction consiste à assurer l'identification et l'authentification des personnes. Parmi les principaux moyens, il est possible de recenser :

- L'authentification par login, mot de passe ;
- L'utilisation d'OTP (One Time Password) ;
- L'authentification par carte à puce (ex: par la carte CPS ou SESAME VITALE) ;
- La biométrie.

- **Gestion des habilitations et contrôle d'accès**

- Gestion des profils ;
- Protection d'accès aux données en fonction du droit d'en connaître ;
- Politique d'Autorisation (PA) émise par le GMSIH.

- Anonymisation de données personnelles

En suivant les recommandations techniques de la norme FD S 97-560.

- **Non Répudiation**

L'obtention de l'assurance de la non-répudiation des actions nécessite de :

- Garantir l'authenticité et l'intégrité de l'élément considéré, par exemple par une signature électronique ;
- Utiliser un tiers de confiance destiné à garantir la qualité de la preuve de non-répudiation.

- **Archivage des données**

L'archivage des données employé dans le cadre des documents électroniques, consiste en l'ensemble des actions permettant de conserver les documents à l'identique dans le long terme. Les problématiques d'archivage légal est tenu à un certain nombre de réglementation, notamment définies dans la loi du 13 mars 2000.

2.3.2 Bonnes pratiques de la sécurité

La norme ISO 27002 :2005 contient onze thèmes destinés à la gestion de la sécurité au sein du système d'information. Chacun de ces thèmes présente les mesures de sécurité correspondantes.

- la gestion de la politique de sécurité elle-même ;
- l'organisation de la sécurité ;
- le contrôle et la classification des biens sensibles (domaines de sécurité, niveaux de sensibilité) ;
- la sécurité du personnel ;

- la sécurité physique ;
- la sécurité des postes de travail ;
- la sécurité des réseaux et des échanges de données ;
- l'administration de la sécurité ;
- les contrôles d'accès logiques et la sécurité des données et des traitements ;
- le développement et la maintenance des systèmes ;
- la gestion des incidents ;
- la continuité de service ;

2.3.3 Synthèse

L'état de l'art présenté ci-dessus introduit la sécurité informatique selon les axes de gouvernance et les axes techniques. Il décrit les normes internationales, les référentiels et standard internationaux, ainsi que les référentiels et standard français.

Le tableau ci-dessous présente la synthèse de l'état de l'art.

Domaines		Normes internationales	Référentiels internationaux	Référentiels français
Gouvernance	Général	ISO27001 ISO27005	Cobit	DGME - RGS DCSSI – EBIOS Clusif- MEHARI
	Médical	ISO20000-1	ITIL CMMI	
Technique	Général	ISO27002 ISO18028 ISO15408 ISO18043	WS-Security RBAC	DGME - RGI DGME - RGS DGME - PRIS V2.1
	Médical	ISO 17090 ISO7816	HL7 IHE DICOM	HPRIM ORBAC OSM

3. CADRE REGLEMENTAIRE

La sécurité de l'information et son cadre légal appliqué à la santé font l'objet de nombreuses lois, décrets et ordonnances qui visent à protéger à la fois les données personnelles, à réglementer l'utilisation d'outils de sécurité, et garantir les droits des patients.

3.1 REGLEMENTATION ET CODES

Les principaux référentiels réglementaires à prendre en compte, dans le cadre de la mise en place de la sécurité informatique dans les établissements de santé :

- Le code de la santé publique art. L1110-4 et L1111 (loi n°2002-303 du 4 mars 2002 relative aux droits des malades et de la qualité du système de santé)

Le code de la santé publique précise dans ces deux articles la définition du secret médical et de la protection des données du malade, ainsi que l'obligation d'information du patient sur les traitements et opérations réalisées et l'obtention de son consentement.

- Le code de la santé publique art. R 1111-13 Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de santé à caractère personnel.
- Circulaire DHOS/F2/2007/248 du 15 juin 2007 - Hôpital 2012

Cette circulaire définit le cadre du plan de modernisation et de mises aux normes des hôpitaux.

- Circulaire DHOS/E1/DAF/DPACI/2007/322 relative au décret n° 2006-6 du 4 janvier 2006 sur la conservation du dossier médical
- Le code de l'assurance maladie (loi n°2004-810 du 13 août 2004 relative à l'assurance maladie).

La loi porte création du dossier médical personnel. La création et la consultation du dossier médical sont conditionnées par l'accord express du patient.

3.2 LOIS INFORMATIQUE ET LIBERTES

La loi Informatique et Libertés définit le cadre légal permettant de protéger les données personnelles traitées au sein du système d'information, ainsi que définit un cadre éthique lié à l'informatisation des systèmes. La CNIL, l'organisme garant de cette loi, émet des délibérations spécifiques à certains contextes (notamment la santé), et détient un droit de veto sur les mises en service d'application traitant de données à caractère personnelles.

- Loi du 6 janvier 1978 et sa modification du 6 août 2004 (loi informatique et libertés)

La CNIL émet plusieurs directives concernant le recueil, le stockage et le traitement d'informations médicales à caractère personnel, afin d'assurer la liberté du patient à exprimer son consentement. En particulier, la CNIL demande à ce que le patient ne soit pas systématiquement pénalisé en terme de remboursement des soins et des services s'il refuse de donner son consentement à la consultation ou à l'échange des informations médicales le concernant.

La modification du 6 août 2004 consiste à la mise en conformité de la loi informatique et libertés avec les directives européennes.

- Délibérations :
 - 81-94 du 21 Juillet 1981

Qui recommande une analyse et évaluation des risques pour tout nouveau système informatique, une sensibilisation du personnel à la sécurité, la mise en place de mesures de protections adéquates, ainsi que la définition d'un responsable de la sécurité du système.

- 01-011 du 08 mars 2001

Indiquant des recommandations de sécurité et de protections des données personnelle, à destination des sites de santé destinés au public.

- 82-028 du 16 mars 1982

Délibération et rappels sur les obligations relatives aux essais et expériences.

3.3 LOIS GENERALES SUR LA SECURITE DE L'INFORMATION

3.3.1 Lois sur la signature électronique et l'usage de la cryptographie

- Loi n°2004-575 du 21 juin 2004, Loi pour la confiance dans l'économie numérique. L'article 33 précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
- Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
- Décret 2002-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
- Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

3.3.2 Loi sur l'archivage légal

- La loi du 13 mars 2000

Qui indique que la signature électronique ayant valeur de preuve, peut être pris en compte dans un cadre d'archivage légal.

3.3.3 Certification des produits de sécurité

- Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organisations qui procèdent à leur évaluation

3.3.4 Lutte contre la fraude informatique

- Loi du 5 janvier 1988 relative a la fraude

La loi du 5 janvier 1988 ou loi « Godfrain », définit certaines infractions et fraudes informatiques, ainsi que les peines encourues.

3.4 LOIS SPECIFIQUES AU MILIEU DE LA SANTE

Les lois et décrets ci-dessous concernent les obligations en matière de sécurité informatique, spécifique au milieu de la santé.

- Décret 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique. Il rend notamment obligatoire l'utilisation de la carte CPS pour toute consultation d'information à caractère personnelle.
- La loi du 30 janvier 2007 (art.25)

L'article prescrit que les règles de confidentialité et de sécurité applicables à ces données seront définies par décret en conseil d'état, pris après avis de la CNIL. Ainsi, le décret n°2007-960 du 15 mai 2007 introduit dans la partie réglementaire du code de la santé publique une nouvelle section 1 sur « la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique » dont les articles R 1110-1 et R 110-2 prévoient que des référentiels spécifiques arrêtés par le ministre de la santé s'imposeront aux professionnels, établissements, réseaux et organisations du système de santé, avec un délai de mise en conformité d'un an à compter de leur date de publication ; ce délai est porté à 3 ans en ce qui concerne l'obligation d'usage d'une carte de professionnel de santé pour accéder en établissements aux informations médicales à caractère personnel (article R 1110-3).

- Loi sur la bioéthique du 1^{er} Juillet 1994

La loi du 1^{er} Juillet 1994, modifie la loi n° 78-17 du 6 janvier 1978, pour préciser les règles concernant le traitement de données nominatives relatives à la santé.

4. RECOMMANDATIONS DU RG*

4.1 RGI : RECOMMANDATIONS / REGLES

Cette partie présente des exemples de règles extraites du RGI concernant les obligations de sécurité décrits avec pour objectif l'interopérabilité des systèmes. Il n'est traité ici que les éléments spécifiques à la sécurité, les autres règles étant traitées dans les différentes fiches du projet. Les problématiques spécifiques à la traçabilité seront traitées dans la fiche AD-HOC.

Règles concernant l'identification et l'authentification des acteurs :

Ci-après un exemple de règles portant sur la notion d'identification, figurant dans la version 0.98b du RGI, volet organisationnel :

RIO 0102 : Il est OBLIGATOIRE que l'identifiant de connexion (login) d'un usager (tous types, toutes populations) soit unique dans le référentiel d'identités utilisé et aussi pérenne que possible : des règles de construction doivent être définies et imposées à cette fin.

... et pour l'acteur « agent » :

RIO 0101 : Il est RECOMMANDE d'évoluer vers l'attribution d'un identifiant de l'Agent unique et stable au sein de sa structure d'appartenance.

RIO 0111 : Il est OBLIGATOIRE que les usagers Agents s'authentifient auprès de leur structure d'appartenance.

Cette dernière règle passera au niveau RECOMMANDE dans la prochaine version du RGI.

...pour l'acteur « professionnel » :

RIO 0112 : Il est RECOMMANDE que l'usager Professionnel qui possède un Gestionnaire d'Identités s'authentifie auprès de celui-ci.

RIO 0114 : Il est OBLIGATOIRE que l'usager Professionnel s'authentifie auprès du Fournisseur de service s'il ne possède pas de Gestionnaire d'Identités

... pour l'acteur « utilisateur du service » :

RIO 0113 : Il est OBLIGATOIRE que les usagers *Particuliers* s'authentifient auprès du Gestionnaire d'Identités mis à disposition par le *Fournisseur de services*.

Règles concernant la fédération d'identité :

Dans le cadre des téléservices, le RGI présentes un certain nombre de règles spécifiques à la mise en place d'un service de SSO à destination des utilisateurs. Le SSO mis en place est basé sur le concept de fédération d'identité.

Dans ce cadre :

RIO 0154 : Il est OBLIGATOIRE d'utiliser un système de fédération d'identité pour la mise en place de systèmes d'authentification unique des usagers dans des téléservices dépendant de différentes administrations.

La fédération d'identité mise en place doit préférentiellement se baser sur les standards définis par le groupement « Liberty Alliance » :

RIO 0156 : Il est RECOMMANDÉ d'utiliser SAML 2.0 ou ID-FF 1.2 pour fédérer des services sur un cercle de confiance inter administrations

RIO 0157 : Il est RECOMMANDÉ d'utiliser ID-WSF 1.1 pour échanger des attributs entre des services fédérés sur un cercle de confiance inter administrations.

Règles concernant l'archivage des données :

Le RGI volet organisationnel précise de même certaines règles destinées à la mise en place d'un service d'archivage dédié à un téléservice et notamment :

RIO 0148 : Il est OBLIGATOIRE, pour que l'archivage électronique remplisse sa finalité juridique, que les modalités mises en place permettent de garantir que le document archivé peut être lu et intelligible, imputable à un auteur identifié et qu'il est fiable et intègre jusqu'au terme du délai durant lequel des droits y afférents peuvent exister

RIO 0149 : Il est RECOMMANDE, pour que l'archivage électronique soit regardé comme fiable d'un point de vue juridique, que les procédures mises en place soient précisément décrites et mises en œuvre

RIO 0150 : Il est RECOMMANDE pour assurer la confidentialité que le service d'archivage mette en place un service sécurisé par un contrôle d'accès et, si nécessaire, un chiffrement des données

RIO 0153 : Il est RECOMMANDE d'établir une « politique d'archivage » avant toute mise en œuvre d'un système d'archivage électronique.

Règles concernant la protection des données personnelles :

Les obligations légales concernant la protection des données personnelles sont déclinées sous forme de règles dans le RGI, volet opérationnel.

RIO 0166 : IL EST OBLIGATOIRE que les responsables des autorités administratives veillent à ce que leurs personnels mettent en œuvre et appliquent, de manière effective, les mesures de confidentialité et sécurité concernant les données personnelles

RIO 0167 : IL est RECOMMANDE que les mots de passe permettant aux usagers et aux agents d'accéder aux informations comportent au moins 8 caractères, dont au moins une lettre minuscule, une lettre majuscule, un chiffre, un caractère non-alphanumérique. Ils doivent être changés au moins tous les deux mois

RIO 168 : IL est INTERDIT que plusieurs personnes au sein d'un même service partagent même mot de passe.

Ces règles font partie des obligations et bonnes pratiques communes à l'ensemble des référentiels et normes de sécurité.

Règles techniques :

Afin de garantir l'interopérabilité des systèmes, le RGI volet technique présente un certain nombre de règles destinées à garantir un niveau de sécurité global et l'interopérabilité des fonctions de sécurité.

Règles relatives à la cryptographie :

RIT0234: Il est OBLIGATOIRE que le format des certificats de personne et de serveur soit conforme au document « Profils de certificats/LCR/OCSP et Algorithmes Cryptographiques » de la « PRIS » Politique de Référencement Intersectorielle de Sécurité V2.1.

RIT0235 : Il est OBLIGATOIRE que les contremarques de temps soient conformes au format défini dans la Politique d'Horodatage Type V2.1. Ce document appartient à l'ensemble documentaire appelé « PRIS » Politique de Référencement Intersectorielle de Sécurité.

RIT0236 : Il est OBLIGATOIRE de respecter les règles et recommandations concernant le choix et le dimensionnement des mécanismes de cryptographie de niveau de robustesse standard, DCSSI, version 1.02 du 19 novembre 2004.

Ces règles rendent obligatoire la conformité avec la PRIS v2.1 au niveau de la gestion des certificats.

Règles relatives aux Web Services :

Les règles suivantes forment la base normative de sécurisation des Web Services.

RIT0069 : Il est RECOMMANDÉ d'utiliser le protocole XML Encryption pour chiffrer des documents XML.

RIT0070 : Il est OBLIGATOIRE d'utiliser la fonction de signature XAdES pour signer des documents XML et de se conformer au profil de signature pour l'administration électronique.

RIT0071 : Il est RECOMMANDÉ d'utiliser la fonction WS-Security pour sécuriser des Web Services.

RIT0090 : Il est RECOMMANDÉ d'utiliser le langage SAML version 2.0 (recommandation UIT-TX.1141) pour les déclarations de données d'authentification et d'autorisation.

Règles de sécurité applicative :

Le RGI volet technique présente des règles de base de sécurisation des transferts de données pour les applications. Les règles suivantes fournissent des normes d'intégration et de développement de service :

RIT0079 : Il est OBLIGATOIRE d'utiliser la méthode HTTP POST, au lieu de la méthode HTTP GET, lors du passage de paramètres à caractère confidentiel ou personnel

RIT0068 : Il est OBLIGATOIRE d'utiliser les protocoles TLS 1.1 ou SSL 3.0 pour sécuriser les échanges s'appuyant sur des protocoles applicatifs tels que FTP, HTTP, IMAP, LDAP, POP3, SIP, SMTP, etc.

4.2 RGS : RECOMMANDATIONS / REGLES

Le RGS traite des exigences et recommandations de sécurité pour l'ensemble des téléservices dédiés à l'administration, et ce notamment pour permettre la mise en conformité des téléservices avec l'ordonnance du 8 décembre 2005.

Le RGS prends en compte deux principaux volets, le volet organisationnel, traitant des règles de gouvernance de la sécurité de l'information, et un volet plus techniques, définissant les règles et obligations autour des fonctions de sécurité.

Les règles de gouvernance s'appuient notamment sur l'ISO 27001, afin de définir le cadre organisationnel et d'amélioration continue de la sécurité. Ainsi :

RS0002 : Il est OBLIGATOIRE de fonder toute réflexion relative à la SSI sur une démarche de gestion des risques afin de rationaliser les prises de décisions. Ceci en effectuant une analyse des risques (EBIOS recommandée).

RS0004 : Il est RECOMMANDÉ de gérer la SSI en amélioration continue, par exemple en mettant en place un « système de management de la sécurité de l'information » (SMSI) tel qu'il est défini dans l'ISO 27001, pour :

Planifier (plan) : définir le cadre du SMSI, apprécier et spécifier le traitement des risques SSI ;

Mettre en œuvre (do) : mettre en place et maintenir les mesures ;

Vérifier (check) : vérifier que les mesures fonctionnent conformément à l'étape Planifier et identifier les améliorations possibles du SMSI ;

Améliorer (act) : étudier et mettre en place les améliorations identifiées pour le SMSI.

RS0006 : Il est OBLIGATOIRE d'élaborer une Politique SSI globale de l'organisme, et, selon les besoins, des Politiques SSI spécifiques (à une direction, à un service, à un système d'information, à un domaine particulier de la SSI...) cohérentes avec la PSSI globale.

RS0009 : Il est OBLIGATOIRE d'apprécier les risques pesant sur un système d'information en préalable à sa définition, et d'identifier les objectifs de sécurité à satisfaire pour offrir des prestations de sécurité conformes aux besoins des autorités administratives et des usagers.

RS0011 : Il est OBLIGATOIRE de définir les exigences de sécurité adaptées aux objectifs de sécurité identifiés pour le système d'information, en fonction de la stratégie de traitement des risques adoptée par l'autorité administrative. Le promoteur d'application (téléservice) doit affecter les exigences aux différents acteurs concernés, et s'assurer de leur prise en compte de manière durable.

RS0013 : Il est OBLIGATOIRE que tout nouveau système d'information ou toute évolution pouvant impacter la sécurité fasse l'objet d'une homologation de sécurité par une autorité d'homologation formellement désignée.

Au niveau technique, le RGS définit des fonctions de sécurité et les exigences spécifiques notamment aux aspects cryptographiques :

Au niveau de l'authentification notamment :

RS0015 : Il est OBLIGATOIRE que les certificats de personne d'authentification soient conformes à la Politique de Certification Type Service Authentification V2.1 de la PRIS

RS0016 : Il est OBLIGATOIRE que les certificats de personne d'authentification et de Signature soient conformes à la Politique de Certification Type Services Authentification et Signature V2.1 de la PRIS

RS0017 : Il est OBLIGATOIRE, pour pouvoir être acceptés par l'ensemble des téléservices requérant des certificats « Agent », « Entreprise » ou « Particulier » d'authentification d'un niveau de sécurité donné, que ces certificats soient référencés en tant que certificats « Agent », « Entreprise » ou « Particulier » d'authentification ou d'authentification et de signature, pour ce niveau de sécurité ou pour un niveau supérieur.

RS0018 : Il est OBLIGATOIRE que les téléservices requérant des certificats « Agent », « Entreprise » ou « Particulier » d'authentification d'un niveau de sécurité donné acceptent tous les certificats référencés en tant que certificats « Agent », « Entreprise » ou « Particulier » d'authentification ou d'authentification et de signature, pour ce niveau de sécurité ou pour un niveau supérieur.

RS0019 : Il est OBLIGATOIRE que les nouveaux téléservices ou toute évolution majeure de téléservice requérant des certificats de personne d'authentification sachent gérer la séparation des usages (authentification, signature) et des tailles de clés RSA ou DH de 2048 bits ainsi que l'algorithme de hachage SHA256.

RS0020 : Il est OBLIGATOIRE que les téléservices annoncent le type de certificat : « Agent », « Entreprise » ou « Particulier », l'usage (authentification ou authentification et signature), et le niveau de sécurité qu'ils acceptent.

RS0021 : Il est OBLIGATOIRE que les autorités administratives installant une nouvelle IGC ou faisant appel à un PSCe pour émettre des certificats de personne à usage d'authentification mettent en place une Politique de Certification compatible avec la Politique de Certification Type Service Authentification V2.1.

RS0022 : Il est OBLIGATOIRE que les Distinguish Names (DN) des certificats « Agent », « Entreprise » ou « Particulier », délivrés par le même émetteur à une même personne soient identiques pour les trois usages : authentification, signature et chiffrement.

RS0023 : Il est OBLIGATOIRE de conserver le même Distinguish Name (DN) lors du renouvellement d'un certificat de personne (sauf exception incontournable comme un changement d'état civil alors que le DN inclut le nom du détenteur, auquel cas il est nécessaire de renouveler tous les certificats comportant le même DN en vertu de la règle RS0022).

RS0024 : Il est OBLIGATOIRE que les certificats « Serveur » soient conformes à la Politique de Certification Type Certificats Serveur V2.1 de la PRIS

Des règles équivalentes sont positionnées pour l'authentification par certificats serveurs, pour la signature électronique et le chiffrement avec l'aide de certificats.

D'autre part, si le RGS, recommande l'authentification par certificat, il présente de même des obligations et préconisations pour l'authentification par OTP, ainsi que par mot de passe statique.

Il contient de même des règles sur la personnalisation des cartes à puces :

RS0060 : Il est OBLIGATOIRE que les sites de personnalisation des dispositifs d'authentification, de signature et/ou de chiffrement respectent les exigences de sécurité spécifiées dans le document « Exigences de sécurité des sites de personnalisation ».

RS0061 : Il est OBLIGATOIRE que les sites de personnalisation qui traitent les dispositifs d'authentification, de signature et/ou de chiffrement émis par une autorité administrative (pour les usagers ou pour ses agents) soient titulaires d'une qualification pour ce service.

RS0062 : Il est RECOMMANDE que les dispositifs d'authentification, de signature et/ou de chiffrement émis par une autorité administrative pour les agents soient personnalisés en respectant les exigences qui sont applicables dans le document : « Exigences de sécurité des sites de personnalisation s'ils sont personnalisés par l'autorité administrative elle-même.

L'ordonnance demandant un accusé d'enregistrement et de réception de la part de l'utilisateur, le RGS définit les règles suivantes :

RS0063 : Il est OBLIGATOIRE que les accusés d'enregistrement ou de réception soient cachetés avec un cachet serveur référencé de niveau au moins égal au niveau *.

RS0064 : Il est OBLIGATOIRE que les accusés d'enregistrement ou de réception soient horodatés avec une contremarque de temps référencée.

RS0065 : Il est OBLIGATOIRE que l'accusé de réception, s'il est différé, reprenne les données d'horodatage de l'accusé d'enregistrement.

RS0066 : Il est OBLIGATOIRE que les accusés d'enregistrement ou de réception soient imprimables. L'impression doit contenir toutes les données qui ont participé au calcul de l'intégrité du document et celles qui assurent l'intégrité.

RS0067 : Il est OBLIGATOIRE d'assurer la traçabilité des accusés d'enregistrement et de réception.

Au niveau des outils de sécurité, le RGS préconise le recours à des produits qualifiés par la DCSSI, et dans l'impossibilité, de conduire une analyse des fonctions de sécurité du produit.

Autres principes :

Les prestataires de service de confiance doivent engager une démarche de qualification des produits de sécurité par rapport à un des profils de protection définis dans le cadre des critères communs.

Les offres et services de sécurité doivent se faire référencer :

RS0071 : Il est OBLIGATOIRE que le PSCo voulant faire référencer une offre de service de sécurité pour un niveau de sécurité donné ait été préalablement qualifié pour cette offre.

RS0072 : Il est OBLIGATOIRE que l'offre de service de sécurité d'un niveau donné d'un PSCo soit conforme aux procédures de référencement en vigueur pour pouvoir être référencée.

RS0073 : Il est OBLIGATOIRE que les téléservices requérant un type de produit à un niveau de sécurité donné acceptent tous les produits de ce type référencés pour ce niveau ou pour un niveau supérieur.

4.3 COMMENTAIRE

Les règles citées sont une illustration des préconisations du RGI et du RGS centralisées par rapport aux principaux concepts de sécurité. L'exhaustivité n'est pas recherchée à ce stade de l'étude. Nous identifions seulement les grandes orientations. Cette présente fiche ne cherche qu'à identifier la démarche générale et les principales règles issues des référentiels généraux. La comparaison exhaustive des référentiels fait l'objet d'une phase ultérieure de ces travaux.

5. RECOMMANDATIONS APPLIQUEES A LA SANTE

5.1 RECOMMANDATIONS GMSIH

Le GMSIH a, en 2003, engagé une démarche de sécurisation des hôpitaux, par le biais du développement d'une politique de sécurité devant-être déclinée dans les établissements de santé, et basée sur l'ISO 17799. Cette démarche s'enrichit de guides de mises en place et d'une démarche d'accompagnement des hôpitaux dans la définition de leur sécurité.

Le GMSIH fournit notamment :

- Politique de sécurité cadre et guide de mise en place
- Politique d'autorisation
- Guide d'autoévaluation de la sécurité
 - Outil d'aide à l'autoévaluation
- Guide d'aide à la mise en place de tableaux de bords
- Profils Fonctionnels de Sécurité
 - Ensemble des besoins déterminés pour un domaine de sécurité et des services de sécurité répondant à ces besoins
- Aides de mise en place de services de sécurité
 - Chiffrement, Signature, Authentification,...

Durant l'année 2006 notamment, 40 établissements de santé ont déclinés leur politique de sécurité avec l'accompagnement du GMSIH, et la démarche s'enrichie de documentations supplémentaires notamment liés aux résultats de cet accompagnement, pour former un kit complet de mise en place.

Il est à noter que l'ISO 17799 ayant été modifiée en 2005, (et renommée ISO 27002), et enrichie d'un chapitre sur la gestion des incidents de sécurité qui ne figure pas dans la norme 17799.

Le GMSIH à d'autre part effectué en 2006 un travail autour de la sécurisation des transferts T2A.

5.2 RECOMMANDATIONS HL7

Le HL7 et l'organisme de suivi du HL7, le HPRIM, préconisent une gestion des habilitations basée sur le modèle RBAC (Role Based Access Control), autour de profils RBAC spécifiques au monde de la santé.

Ces profils permettent de définir des règles d'autorisation et de contrôles d'accès spécifiques aux métiers de la santé.

5.3 MODELE ORBAC

Le modèle OrBAC, créé dans le cadre du projet RNRT MP6 (Modèles et Politiques de Sécurité des Systèmes d'Informations et de Communication en Santé et en Social), définit un modèle de contrôle d'accès destiné à compléter et remplacer le modèle RBAC pour le milieu de la santé.

OrBAC propose un modèle abstrait permettant de gérer une politique de contrôle d'accès fondé sur une organisation générale plutôt qu'un rôle.

Il permet de mettre en place des contrôles d'accès spécifiques pouvant dépendre d'un contexte changeant (par ex : le contexte d'urgence en hôpital), des organisations spécifiques au milieu de la santé, ainsi que de prendre en compte la délégation et la hiérarchisation des droits.

Il s'accompagne d'un guide d'administration du modèle : AdOrBAC, ainsi que d'un outil Opensource de gestion de la politique : MotOrBAC.

5.4 RECOMMANDATIONS IHE

Le modèle IHE définit un certain nombre de profils destinés à la gestion des systèmes d'informations en établissement de santé. Les principaux profils touchant à la sécurité sont les suivants :

- Exigences globales de sécurité via les profils suivants:
- Gestion de l'audit et de l'authentification des nœuds réseau : Audit Trail and Node Authentication (ATNA)
- Gestion de l'horodatage: Consistent Time (CT)
- Autorisation de participation par l'utilisateur : Basic Patient Privacy Consents (BPPC)
- Système d'authentification : Enterprise User Authentication (EUA)
- Fédération d'identité : Cross-Enterprise User Assertion (XUA)
- Annuaire pages blanches : Personnel White Pages (PWP)
- Signature électronique : Digital Signatures (DSG)
- Contrôles d'intégrité spécifiques sur le partage de document (XDS, XDM, XDR)

Opérationnellement, cette approche est peu mise en place en France, notamment, dans les établissements de santé de plus petite taille (exigences de serveurs de traces).

5.5 REFERENTIELS TECHNIQUES SPECIFIQUES

5.5.1 Homologation OSM

Le référentiel d'homologation OSM permet de définir les règles principales de sécurité à destination des outils de sécurisation de la messagerie utilisant la carte CPS.

Il présente notamment les exigences suivantes :

- Echanges sécurisés via S/MIME
- Exigences techniques autour des standards de chiffrement utilisés, via un profil cryptographique :
 - 3DES (chiffrement symétrique);
 - RSA (ex: pour la signature via CPS)
 - Gestion des clefs et des certificats (publication des CRLs)

5.5.2 Sécurisation DICOM

Les échanges d'images médicales utilisant le standard DICOM peuvent être sécurisés via l'utilisation des standards suivants :

- Mise en place de sécurisation principalement au niveau flux:
 - Canaux chiffrés
 - Conservation de l'intégrité des données durant le transport
 - Authentification des entités
 - Modes de chiffrement:
 - TSL 1.0
 - ISCL (standard japonais, cryptographie basée sur DES à faibles tailles de clefs).
- Enveloppe CMS pour chiffrer :
 - Certificats X509
- Signature du message (signature RSA)
- Mise en place d'anonymisation des messages

6. CONCLUSIONS

Convergence des référentiels :

Les règles du RGI et du RGS ont été créées pour cadrer les échanges avec les administrations et les autorités administratives. Les échanges des établissements de santé et des réseaux de santé doivent donc respecter ces règles dans le champ concerné. Il s'agit principalement de pratiques normalisées d'autre part dans les normes internationales (par ex : ISO 27001). Les règles sont de deux types :

- Règles de gouvernance sécurité :

Ces règles, définies dans le RGS, et l'ISO 27001 sont applicable à priori à l'ensemble des établissements. L'accompagnement effectué actuellement par le GMSIH autour des politiques de sécurité renforcent d'ailleurs ce principe et constituent une base de mise en place d'un SMSI.

Une adaptation opérationnelle de ces règles en fonction des différents environnements est un élément qui doit toutefois être pris en compte de manière à adapter la sécurité aux moyens de l'établissement concerné. Ce niveau d'exigence adaptable peut notamment se traduire par le choix d'un niveau d'exigence PRIS spécifiquement choisis par les téléservices de santé.

Ces règles générales sont également reprises par la HAS, qui dans ses critères d'homologation des établissements, intègre la vérification de certaines obligations de gouvernance, comme l'obligation de mise en place d'une politique de sécurité, en cohérence avec les travaux du GMSIH.

L'étude effectuée en 2003 par le GMSIH autour de la sécurité des établissements de santé est d'autre part conforme avec l'ISO 17799 :2000. La version 2005 de l'ISO 27002 intègre la gestion des incidents, qui ne se retrouve donc pas dans la

- Règles techniques de sécurité :

De nombreux référentiels techniques existent dans le milieu de la santé. Certains sont poussés par des industriels de santé, d'autres de fournisseurs de services déjà en place. Le cadre légal lui-même intègre des exigences de sécurité qui impactent directement les mises en places techniques.

L'applicabilité de ces lois et règlements est parfois difficile notamment à cause des contextes complexes. Une solution technique acceptable pour un établissement de santé de grande taille ne sera pas forcément acceptable dans le cadre de la médecine de ville ou dans un établissement de santé de petite taille.

Les enjeux principaux de sécurité du monde de la santé visent à protéger le patient et le professionnel de santé de manière à assurer les soins les plus appropriés.