ECOLE NATIONALE SUPERIEURE D’INFORMATIQUE

POLITIQUE DE SECURITE DU SYSTEME D’INFORMATION HOSPITALIER (SIH)

Réalisé par :

* MAAMAR KOUADRI Wissam (G05)
* OUAIL Roumeissa (G08)
* RAHMOUNE Zakia (GO8)
* ZERROUK Asmaa (G06)

Encadré par :

* Monsieur ANANE

2013 - 2014

Sommaire

[Sommaire 1](#_Toc384706849)

[1. Introduction : 4](#_Toc384706850)

[1.1. La démarche adoptée : 4](#_Toc384706851)

[1.2. Quelques définitions : 4](#_Toc384706852)

[1.2.1. Information : 4](#_Toc384706853)

[1.2.2. Système d’information automatisé : 5](#_Toc384706854)

[1.2.3. Sécurité de l’information : 5](#_Toc384706855)

[1.2.4. Politique de Sécurité des Systèmes d’Information d’un établissement de santé : 5](#_Toc384706856)

[2. Politique de Sécurité Cadre des Systèmes d’Information (PSC-SI) 6](#_Toc384706857)

[2.1. Partie 1 : Fondements de la politique 6](#_Toc384706858)

[2.1.1. Définition de la a Politique de Sécurité Cadre pour les Systèmes d’Information des établissements de santé (PSC-SI) 6](#_Toc384706859)

[2.1.2. Finalités de la Politique de Sécurité Cadre pour les Systèmes d’Information des établissements de santé (PSC-SI) 6](#_Toc384706860)

[2.1.3. Légitimité éthique et déontologique de la sécurité de l’information 7](#_Toc384706861)

[2.2. Partie 2 : Principes et règles de mise en œuvre 7](#_Toc384706862)

[2.2.1. L’ISO 8](#_Toc384706863)

[2.2.2. La Norme ISO 17799 8](#_Toc384706864)

[2.3. Partie 3 : Guide d’élaboration d’une Politique de Sécurité interne 8](#_Toc384706865)

[3. Politique d’autorisation : 9](#_Toc384706866)

[3.1. Définition de l’autorisation : 9](#_Toc384706867)

[3.2. Les objectifs de l’étude : 9](#_Toc384706868)

[3.3. Modélisation fonctionnelle et organisationnelle : 9](#_Toc384706869)

[3.3.1. Contexte métier et besoins : 9](#_Toc384706870)

[3.3.1.1. Définition du SIH : 9](#_Toc384706871)

[3.3.1.2. Les activités exercées dans l'établissement de santé : 9](#_Toc384706872)

[3.3.1.3. Contexte d'accès aux informations selon la situation du patient : 10](#_Toc384706873)

[3.3.2. Concepts fondamentaux du modèle d'autorisation : 10](#_Toc384706874)

[3.3.3. Principes de classification des informations : 11](#_Toc384706875)

[3.3.3.1. Les niveaux de classification : 11](#_Toc384706876)

[3.3.4. Les modèles d'autorisation : 12](#_Toc384706877)

[3.3.4.1. Modèle simple : 13](#_Toc384706878)

[3.3.4.2. Modèle intermédiaire : 14](#_Toc384706879)

[3.3.4.3. Modèle complet : 15](#_Toc384706880)

[3.3.5. Scénarios de gestion du contrôle d'accès logique : 16](#_Toc384706881)

[3.3.5.1. Ouverture de session : 16](#_Toc384706882)

[3.3.5.2. Accès à une ressource : 16](#_Toc384706883)

[3.3.6. Modalités d'administration des autorisations : 17](#_Toc384706884)

[3.3.6.1. Principe d'administration des autorisations : 17](#_Toc384706885)

[3.3.6.2. Scénarios d'administration des autorisations : 17](#_Toc384706886)

[3.3.6.3. Modèles d'organisation pour l'administration des autorisations : 17](#_Toc384706887)

[3.3.6.3.1. Définition des rôles : 17](#_Toc384706888)

[3.3.6.3.2. Attribution des rôles aux utilisateurs : 18](#_Toc384706889)

[3.4. Principes et règles de gestion 19](#_Toc384706890)

[3.4.1. Politique d’autorisation 19](#_Toc384706891)

[3.4.1.1. Principe général 19](#_Toc384706892)

[3.4.2. Gestion du contrôle d’accès logique : 20](#_Toc384706893)

[3.4.2.1. Principe : Concepts élémentaires : 20](#_Toc384706894)

[3.4.2.2. Principe : Mutualisation de l’infrastructure du contrôle d’accès logique 20](#_Toc384706895)

[3.4.2.3. Principe : Gestion des authentifiants 21](#_Toc384706896)

[3.4.2.4. Principe : Ouverture d’une session : 22](#_Toc384706897)

[3.4.3. Traçabilité des accès : 23](#_Toc384706898)

[3.4.3.1. Principe : Génération des traces dans l’administration des autorisations : 23](#_Toc384706899)

[3.4.3.2. Principe : Traçabilité en accès exceptionnel 24](#_Toc384706900)

[3.4.4. Administration des autorisations et supervision du contrôle d’accès 24](#_Toc384706901)

[3.4.4.1. Principe : Gestion des droits par rôles génériques 24](#_Toc384706902)

[3.4.4.2. Principe : Définition des rôles 24](#_Toc384706903)

[3.4.4.3. Principe : Création des comptes des utilisateurs 25](#_Toc384706904)

[3.4.4.4. Principe : Attribution de droits aux utilisateurs 26](#_Toc384706905)

[3.4.4.5. Principe : Mise à jour et révocation des droits des utilisateurs 26](#_Toc384706906)

[3.4.4.6. Principe : Règles de supervision du contrôle d’accès 26](#_Toc384706907)

[3.5. Conclusion 27](#_Toc384706908)

[4. Autoévaluation : 28](#_Toc384706909)

[4.1. Introduction : 28](#_Toc384706910)

[4.2. Définition de l’auto-évaluation : 28](#_Toc384706911)

[4.2.1. Les objectifs d’un guide d’auto-évaluation : 28](#_Toc384706912)

[4.2.2. Cycle de vie de l’auto-évaluation d’un établissement : 29](#_Toc384706913)

[4.3. Présentation du guide d’auto-évaluation : 30](#_Toc384706914)

[4.3.1. Fonctionnement du logiciel : 30](#_Toc384706915)

[4.3.1.1. 1-Questionnaire d’auto-évaluation  (étape d’évaluation): 30](#_Toc384706916)

[4.3.1.2. L’état du lieu : 31](#_Toc384706917)

[4.3.1.3. Le degré de couverture : 31](#_Toc384706918)

[4.3.1.3.1. Table de menace prédéfinie : 33](#_Toc384706919)

[4.3.1.4. Efficacité des principes (classification des principes par priorité): 35](#_Toc384706920)

[4.3.1.5. Priorités d’action : 36](#_Toc384706921)

[4.3.1.6. Ordonnancement : 37](#_Toc384706922)

[5. Conclusion : 38](#_Toc384706923)

[6. Glossaire 39](#_Toc384706924)

[7. Annexe : 40](#_Toc384706925)

[7.1. Règles du principe : 40](#_Toc384706926)

[7.2. Les rôles des PS : 50](#_Toc384706927)

[7.2.1.1. Médecin unité de soins : 50](#_Toc384706928)

[7.2.1.2. Brancardiers : 50](#_Toc384706929)

[7.2.1.3. Pharmaciens : 50](#_Toc384706930)

[7.2.1.4. Aides-soignants et agents hospitaliers : 51](#_Toc384706931)

[7.2.1.5. Cadres médico-techniques de radiologie : 51](#_Toc384706932)

[7.3. Les scénarios de la gestion d’accès logique : 52](#_Toc384706933)

[7.3.1. Modification des rôles activés : 52](#_Toc384706934)

[7.3.2. Clôture de session : 52](#_Toc384706935)

[7.3.3. Accès à une ressource par exception au contrôle d’accès : 52](#_Toc384706936)

[7.4. Les scénarios d’administration des autorisations : 52](#_Toc384706937)

[7.4.1. Création du compte d’un utilisateur interne : 52](#_Toc384706938)

[7.4.2. Création du compte d’un intervenant externe : 52](#_Toc384706939)

[7.4.3. Suppression d’un compte : 53](#_Toc384706940)

[7.4.4. Définition des rôles : 53](#_Toc384706941)

[7.4.5. Affectation d’un utilisateur à un élément de structure avec un rôle : 53](#_Toc384706942)

[8. Référence 54](#_Toc384706943)

[9. Webographie 54](#_Toc384706944)

1. Introduction :

Aujourd’hui, les établissements et les professionnels de  santé  doivent coopérer afin d’assurer une prise en charge des patients, qui s’inscrit dans une continuité sanitaire et sociale. L'enjeu est majeur puisqu’il s’agit de favoriser l'évolution des pratiques médicales vers une médecine coopérative, plus organisée, davantage coordonnée autour du patient, permettant de simplifier et d'optimiser le parcours de celui-ci dans le système de soins.

La construction de systèmes d’information et de communication centrés sur les dossiers de santé et sur la production des soins, au service de l’échange et du partage de l’information de santé, dans le respect des droits du patient, contribue à la mise en œuvre et à l’efficacité de ces nouvelles formes d’organisation et de coopération.

Dans ce contexte, la sécurité des systèmes d’information constitue l’un des éléments essentiels pour instaurer un climat de confiance qui favorise l’échange et le partage de données de santé à caractère personnel.

* 1. La démarche adoptée :

La sécurité des systèmes d’information relève :

1. D’un corpus de bonnes pratiques, qui reflète l’état de l’art en matière de services de sécurité à mettre en œuvre : ainsi la Politique de Sécurité Cadre (PSC-SI), sur le modèle normalisé ISO 17799, présente un cadre de référence pour la mise en place de la sécurité du ou des systèmes d’information d’un établissement.
2. D’une Politique d’Autorisation (PA), déclinaison de la politique de sécurité, dont l’objectif est de faire respecter la confidentialité, l’intégrité et la traçabilité des informations médicales nominatives, au travers d’une gestion rigoureuse des habilitations.
3. D’une auto -évaluation de la sécurité du système d’information (Guide d’auto -évaluation), par rapport à la PSC-SI pour les établissements de santé, indiquant les priorités pour la mise en conformité de la sécurité du SIH  et qui se complète par un plan d’action permettant de décliner les principes et priorités retenus.
   1. Quelques définitions :

Afin d’appréhender la portée de la politique de sécurité, il convient de rappeler quelques définitions :

* + 1. Information :

Au sein de l’établissement de santé, l’information constitue un « actif » essentiel pour le patient, l’organisation des soins et la prise en charge par les services : elle doit donc être protégée de manière appropriée.

L’information se présente sous de multiples formes : imprimée ou écrite sur papier, orale, stockée sur des supports électroniques, transmise par la poste, par un réseau électronique ou par un réseau téléphonique, montrée sur des images médicales, des films, des supports de visioconférence.

* + 1. Système d’information automatisé :

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

* + 1. Sécurité de l’information :

La sécurité de l’information est caractérisée comme étant la préservation de :

1. Sa confidentialité : faire en sorte que l’information ne soit accessible qu’aux personnes autorisées à y accéder.
2. Son intégrité : protéger l’exactitude et l’intégrité de l’information et des méthodes de traitement.
3. Sa 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.
4. Les moyens de preuve et contrôle nécessaires aux utilisateurs pour accorder leur confiance dans l’information fournie.
   * 1. Politique de Sécurité des Systèmes d’Information d’un établissement de santé :

« L’ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les biens, en particulier les informations médicales sensibles, au sein d’un établissement de santé et lors de ses communications avec d’autres systèmes d’information de santé ou d’autres professionnels de santé (réseaux de santé, praticiens libéraux, autres établissements) ».

1. Politique de Sécurité Cadre des Systèmes d’Information (PSC-SI)

La PSC-SI est composée de trois parties :

1. Partie 1 : Fondements de la Politique de Sécurité
2. Partie 2 : Principes et règles de mise en œuvre
3. Partie 3 : Guide de rédaction de la politique de sécurité des systèmes d’information de l’établissement
   1. Partie 1 : Fondements de la politique

La première partie présente les fondements de la Politique de Sécurité Cadre des Systèmes d’Information : définition principale et finalités.

* + 1. Définition de la a Politique de Sécurité Cadre pour les Systèmes d’Information des établissements de santé (PSC-SI)

La PSC-SI est l’ensemble des principes de sécurité juridiques, humains, organisationnels et techniques qu’il est recommandé de mettre en œuvre au sein de l’établissement de santé et lors de ses changes avec les autres systèmes d’information de santé ou avec les autres professionnels de santé (réseaux, praticiens libéraux, autres établissements).

* + 1. Finalités de la Politique de Sécurité Cadre pour les Systèmes d’Information des établissements de santé (PSC-SI)

Les finalités de la politique de sécurité cadre sont les suivantes :

1. Sensibiliser aux risques qui menacent l’information et les systèmes d’information des établissements de santé, ainsi qu’aux moyens disponibles pour s’en prémunir.
2. Créer un cadre général, adapté aux systèmes d’information hospitaliers, pour aider les personnes chargées d’élaborer et de mettre en œuvre des mesures, des consignes, des procédures cohérentes, en vue d’assurer la sécurité de l’information et du système d’information automatisé.
3. Promouvoir la coopération entre les différents services et acteurs de l’établissement pour l’élaboration et la mise en œuvre de ces mesures, consignes et procédures.
4. Susciter la confiance des utilisateurs et des patients dans le système d’information automatisé.
   * 1. Légitimité éthique et déontologique de la sécurité de l’information

Les principes et les règles de la Politique de Sécurité des Systèmes d’Information s’appuient sur la déontologie des activités médicales :

1. La sécurité de l’information est généralement associée dans le monde de la santé au respect du secret professionnel « couvre tout ce qui est venu à la connaissance du médecin dans l’exercice de sa profession, c’est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu’il a vu, entendu ou compris ».
2. Lorsqu’il devient « hébergeur » de dossiers médicaux, l’établissement de soins inclut dans sa politique de sécurité les dispositions organisationnelles et techniques lui permettant de respecter la vie privée (anonymat du patient).
   1. Partie 2 : Principes et règles de mise en œuvre

La deuxième partie propose au responsable de l ‘élaboration de la Politique de Sécurité de l’établissement le choix parmi 39 principes déclinés en 168 règles. Elle est articulée autour de 10 chapitres :

1. Chapitre 1 : Politique de sécurité
2. Chapitre 2 : Management de la sécurité
3. Chapitre 3 : Inventaire et classification des ressources
4. Chapitre 4 : Sécurité et ressources humaines
5. Chapitre 5 : Sécurité physique et sécurité de l’environnement
6. Chapitre 6 : Exploitation informatique et gestion des réseaux
7. Chapitre 7 : Contrôle d’accès logique
8. Chapitre 8 : Développement et maintenance des applications et des systèmes
9. Chapitre 9 : Gestion de la continuité
10. Chapitre 10 : Respect de la réglementation interne et externe

Chaque chapitre comprend des principes de sécurité.

Chaque principe est documenté de la manière suivante :

1. Intitulé du principe
2. Objectif du principe
3. Correspondance du principe avec la norme ISO 17799
4. Règles du principe (Voir annexe [7.1](#règlesduprincipe))
   * 1. L’ISO

L'Organisation Internationale de Normalisation « ISO » est un [organisme de normalisation](http://fr.wikipedia.org/wiki/Organisme_de_normalisation) international composé de représentants d'organisations nationales de normalisation de 164 pays. Cette organisation créée en [1947](http://fr.wikipedia.org/wiki/1947) a pour but de produire des [normes](http://fr.wikipedia.org/wiki/Normes_et_standards_industriels) internationales dans les domaines industriels et commerciaux appelées [normes ISO](http://fr.wikipedia.org/wiki/Liste_de_normes_ISO).

* + 1. La Norme ISO 17799

La norme ISO/CEI 17799 est une norme internationale concernant la [sécurité de l'information](http://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_de_l%27information), publiée en décembre 2000 par l'[ISO](http://fr.wikipedia.org/wiki/Organisation_internationale_de_normalisation) dont le titre est « Code de Bonnes Pratiques pour la Gestion de la Sécurité d'Information ».

La deuxième édition de cette norme a été publiée en juin 2005, elle comporte un nouveau chapitre : « Analyse des Risques ». Cette deuxième édition a changé de numéro de référence en juillet 2007. Il s'agit maintenant de la norme [ISO/CEI 27002](http://fr.wikipedia.org/wiki/ISO/CEI_27002).

* 1. Partie 3 : Guide d’élaboration d’une Politique de Sécurité interne

La troisième partie indique la démarche à suivre par l’établissement pour rédiger sa propre politique en s’appuyant sur le contenu de la politique de sécurité cadre :

1. Première étape : désignation d’un rédacteur et constitution du comité de sécurité
2. Deuxième étape : Identification des fondements de la politique de sécurité de l’établissement
3. Troisième étape : Sélection des principes et première rédaction des règles à intégrer à la politique de sécurité de l’établissement
4. Quatrième étape : Validation de la politique de sécurité
5. Cinquième étape : Diffusion de la politique de sécurité

Révision de la politique de sécurité.

1. Politique d’autorisation :
   1. Définition de l’autorisation :

Une **autorisation** est « l’attribution de droits, comprenant la permission d’accès sur la base de droits d’accès ». [[1]](#ISO1)

L’**habilitation** est « le droit accordé à un individu d’accéder à des informations dont le niveau de sécurité est inférieur ou égal à un niveau déterminé ». [[2]](#ISO2)

La politique d’autorisation est la politique qui permet de faire la modélisation fonctionnelle et organisationnelle d’un SI afin de déterminer les différents rôles et personnels du système et leurs attribuer des droits, pour sécuriser l’ensemble des ressources du SI, donc cette politique prend en considération les particularités du milieu d’un SI donné, dans notre cas, il s’agit du milieu hospitalier, tout en s’appuyant sur les habilitations.

* 1. Les objectifs de l’étude :

Dans cette partie du document, on essaie de couvrir un ensemble d’objectifs pour assurer une harmonisation des pratiques de gestion et d’administration du contrôle d’accès logique pour l’ensemble des applications du SIH (système d’information hospitalier). On garantit :

* La **qualité** et la **pérennité** de la sécurité d’accès au SI par l’identification des rôles par métier et l’attribution des permissions d’accès aux personnes via ces rôles ;
* L’**imputabilité** des opérations à leurs auteurs par l’attribution des droits d’accès aux personnes (son tenir compte des rôles qu’elles occupent) ;
* La **rigueur** dans l’attribution des droits ;
* La **protection** des accès lors de l’ouverture du SIH sur d’autres SI.
  1. Modélisation fonctionnelle et organisationnelle :
     1. Contexte métier et besoins :
        1. Définition du SIH :

Le SIH c'est le système qui s'occupe de la gestion d'informations du domaine de santé qui sont accessibles (partage/échange) par les utilisateurs de l'établissement de santé (professionnels de santé, patients, organismes..) ayant des responsabilités et des centres d'intérêt différents. Ce système assure : la communication, le traitement, le stockage et l'archivage des informations liées aux patients.

* + - 1. Les activités exercées dans l'établissement de santé :

Afin de pouvoir appliquer la notion d'habilitation, on a recensé les différentes catégories de professionnels de santé (PS) dans l'établissement : *(La liste n'est pas exhaustive, elle est donnée à titre illustratif)*

* + Médecin unité de soins
  + Infirmière
  + Secrétaire médicale unité de soins
  + Médecin médio-technique
  + Technicien de laboratoire
  + Cadres médio-technique de radiologie
  + Technicien en radiologie (manipulateur)
  + Secrétaire de radiologie
  + Aide-soignant et agent hospitalier
  + Brancardier
  + Pharmacien
  + Préparateur de pharmacie
  + Médecin de ville

Quelques rôles de chaque catégorie sont cités en annexe (Voir annexe [7.2](#roles)).

* + - 1. Contexte d'accès aux informations selon la situation du patient :

Dans plusieurs cas, la situation du patient détermine les règles de l’accessibilité à son dossier médical par les PS. On distingue 5 cas :

1. Patient hospitalier : les PS du service d'hospitalisation doivent avoir accès à tout ou partie de son dossier médicale en plus des informations de séjours à l'exception des informations hautement confidentielles.
2. Patient en consultation : Selon les dates des rendez-vous données aux patient, une fenêtre temporelle est calculée pour permettre au PS d'accéder aux informations dont il a besoin.
3. Patient en service d'urgence : puisque le patient est dans une situation critique, alors les PS de ce service ont accès à l'ensemble du dossier du patient.
4. Recours au conseil d'un autre praticien : le praticien sollicité doit avoir accès au dossier du patient.
5. Accès par un médecin médio-technique (radiologie, laboratoire, service d'anesthésie...) : les médecins du service concerné ont droit d'accéder au dossier médical du patient sur une fenêtre temporelle.
   * 1. Concepts fondamentaux du modèle d'autorisation :

Le modèle proposé dans la politique d'autorisation est une adaptation et une extension des principes du modèle RBAC (Role Based Access Control). En plus de la notion de rôle, les notions suivantes sont nécessaires pour le contrôle d'accès du SIH :

* + Contenu sémantique du dossier médical : le dossier médicale du patient contient des informations qui sont particulièrement confidentielles ce qui y limite l'accès par quelques PS.
  + Structure d'affectation : le praticien est affecté à une unité fonctionnelle (UF) et il ne doit avoir accès qu'aux dossiers dont il a besoin au sein de son UF (exemple : laboratoire, pharmacie...).
  + Mode et lieu d'accès : Certaines informations sur le patient ne sont accessibles qu'à partir d'un endroit précis.
  + Temps : les permissions d'accès sont restreintes à une fenêtre temporelle liée à la présence du patient dans le service ou les dates des rendez-vous.
  + Restriction d'accès à certains dossiers : un PS ne doit accéder qu'aux dossiers des patients dont il a la charge.
  + Le patient peut exprimer une opposition à certains PS d'accéder à son dossier, ou donner une autorisation à des PS externes à l'établissement pour traiter son cas et accéder à son dossier.

Le modèle permettra de tenir comptes des délégations de pouvoir (au sein ou en dehors des équipes). Il prévoit aussi les exceptions avec les contraintes de traçabilité et justifications adéquates pour éviter les abus.

* + 1. Principes de classification des informations :
       1. Les niveaux de classification :

Afin de structurer les autorisations, il est proposé de classifier les éléments du dossier du patient. Trois types de classifications s'imposent : classification selon le degré de confidentialité, classification selon le degré d'intégrité, et classification selon les traces et les contrôle. Les tableaux suivants résument les niveaux de chaque classification.

|  |  |  |
| --- | --- | --- |
| Niveau | Confidentialité | |
| 1 | **Public :** Les informations peuvent être lues par tous | |
| 2 | **Restreint :** Les informations sont lues par des personnes connues et contrôlées | |
| 3 | **Secret médical et professionnel :** Les informations sont protégées par le secret médical ou le secret professionnel et par la législation sur les données à caractère médical | **Données nominatives non médicales :** Les informations sont protégées par la législation sur la protection des données nominatives |
| 4 | **Haute protection :** Domaines du dossier médical dont la transmission est particulièrement restreinte pendant toute la durée de vie ou période de validité car sa divulgation à des personnes non autorisées peut entraîner un préjudice majeur pour le patient. | |

Tableau 1 : Confidentialité

|  |  |
| --- | --- |
| Niveau | Intégrité |
| 1 | **Signalement :** La perte d’intégrité momentanée des informations est acceptée, sous réserve qu’elle soit signalée et ne remette pas en cause le service fourni. Exemple : informations de situation administrative. |
| 2 | **Signalement et correction :** Perte tolérée si signalée et corrigée dans un délai suffisant pour ne pas avoir de conséquence grave sur le service fourni. Exemple : intégrité des informations administratives sauf identification. |
| 3 | **Justification a posteriori :** Les informations doivent rester intègres pendant la période d’utilisation ; toute perte en dehors de la période d’utilisation doit être signalée et corrigée ; si la perte d’intégrité est constatée pendant la période d’utilisation, le service ou traitement est arrêté jusqu’au rétablissement de l’intégrité. Exemple : informations du dossier médical, identification. |
| 4 | **Certification a priori :** Les informations sont certifiées intègres pendant toute leur durée de vie ou leur période de validité. Exemple : données d’identification et d’authentification du professionnel de santé (certification CPS). |

Tableau 2 : Intégrité

|  |  |
| --- | --- |
| Niveau | Preuve et contrôle |
| 1 | **Faible :** Les traces sont faibles et non immédiatement disponibles. |
| 2 | **Auditable :** Les traces des opérations existent et peuvent être rendues disponibles. |
| 3 | **Preuve interne :** Fourniture d’une preuve opposable (mais contestable). |
| 4 | **Preuve externe :** Fourniture d’une preuve incontestable. |

Tableau 3 : Preuve et contrôle

* + 1. Les modèles d'autorisation :

On propose 3 modèles d'autorisation qui se complètent progressivement : simple, intermédiaire et complet. Le modèle complet est le modèle cible, alors que les deux premiers n'ont font que des étapes. (Ces trois modèles sont représentés par des diagrammes de classe)

* + - 1. Modèle simple :

Ce modèle est basé sur l'attribution des droits d'accès par métier.

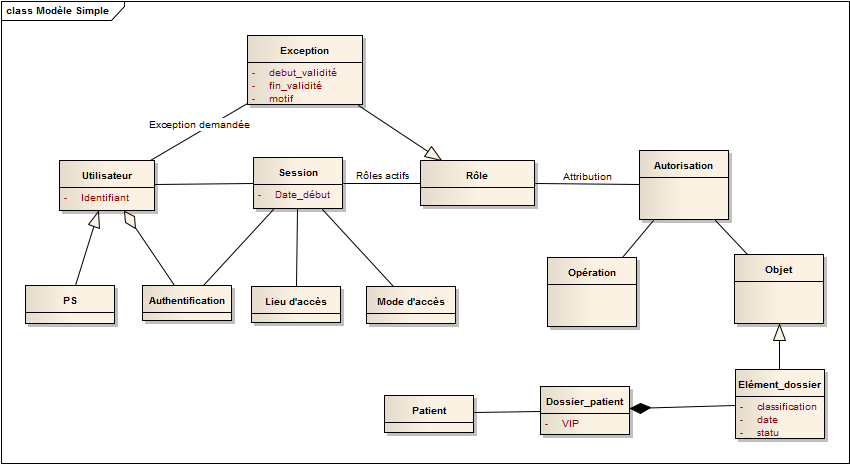


Figure 1 : le modèle simple

Description du modèle :

Une *autorisation* c'est un ensemble d'opérations effectuées sur un objet. Cet objet représente un élément du dossier du patient, un planning ou un rendez-vous.

Un *rôle* est l'ensemble des autorisations attribué à un métier (fonction).

L'*utilisateur* lorsqu'il se connecte au SI par une *authentification*, il accède à une *session* qui regroupe l'ensemble des rôles dont il a accès selon son authentification, le lieu d'accès ainsi que le mode d'accès. L'utilisateur peut éventuellement faire une demande d'autorisation d'accès exceptionnelle, qui lui sera attribuée selon le mécanisme de dérogation.

* + - 1. Modèle intermédiaire :

Ce modèle prend en considération les structures de l'établissement en plus des différents métiers.

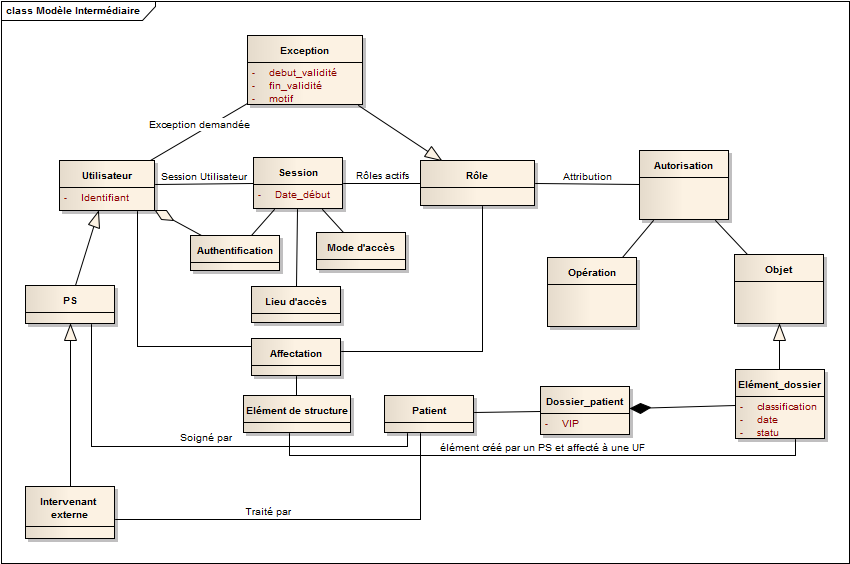


Figure 2 : Le modèle intermédiaire

Description du modèle :

Par rapport au modèle simple, on rajoute la notion d'affectation qui relie un utilisateur à une structure par un rôle.

Le modèle montre aussi que le patient peut donner des autorisations à un PS ou à un intervenant externe de voir son dossier médical (le modèle permet de récupérer les listes des PS et intervenants externes autorisés).

L'exception dans ce modèle est considérée comme un rôle qui peut être affecté à un utilisateur temporairement.

* + - 1. Modèle complet :

Ce modèle sert les établissements ayant des contraintes d'accès logique complexes. Il ajoute par rapport au modèle intermédiaire les éléments nécessaires pour le suivi de la trajectoire du patient.

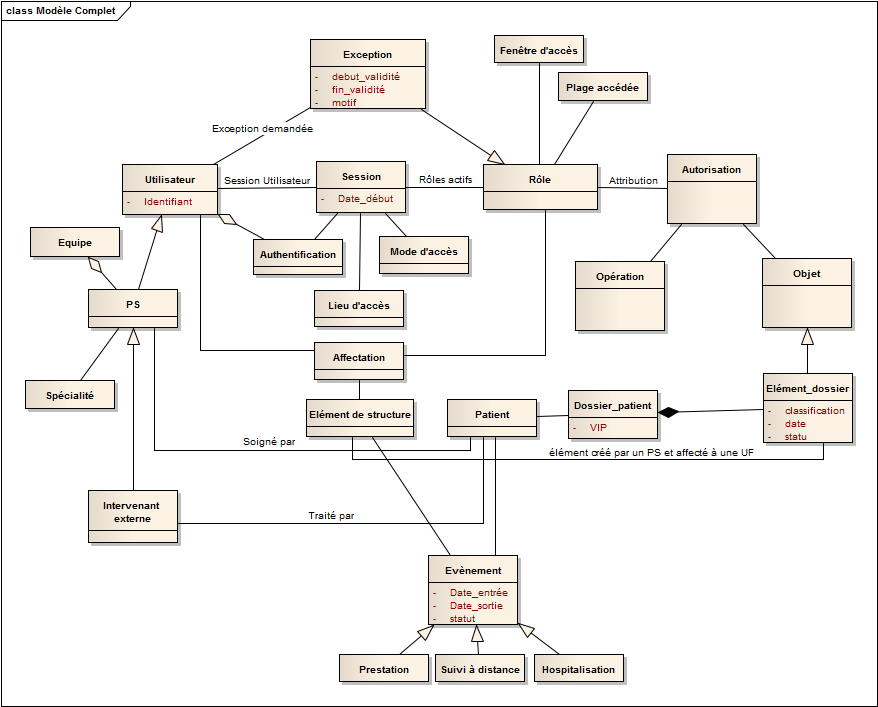


Figure 3 : Le modèle complet

* + Notion de trajectoire du patient :

Elle a pour vocation de permettre, pour certains PS, de restreindre l'accès au dossier du patient à certaines périodes temporelles. On distingue deux notions :

- **La fenêtre d'accès :** c'est la période pendant laquelle le PS peut accéder au dossier;

- **La plage accédée :** correspond aux informations auxquelles le PS à accès.

Les périodes temporelles sont définies par des évènements qui ont une date de début et une date de fin. Exemples d'évènement : hospitalisation, demande de prestation (consultation, analyses, actes d'imagerie...). Ces évènement peuvent être déclenchés sans que le patient soit présent (exemple : suivi des dossiers des patients dans un traitement de cancérologie).

* + Contrainte du modèle complet :
* Contenu sémantique du dossier médical :
  + **Haute protection :** les éléments du dossier classés "haute protection" requièrent un niveau d'habilitation précis.
  + **VIP :** les dossiers classés "VIP" ne peuvent être accédés que par les PS traitant ces patients.
* Structure d'affectation : le PS ne peut accéder au dossier que si ce dernier appartient à son UF (unité de fonction), ou s'il possède une exception approuvée par le mécanisme de dérogation.
* Temps : les droits d'accès sont restreints à une fenêtre temporelle.
  + 1. Scénarios de gestion du contrôle d'accès logique :

Afin de faciliter l'utilisation des modèles, on détaille quelques scénarios :

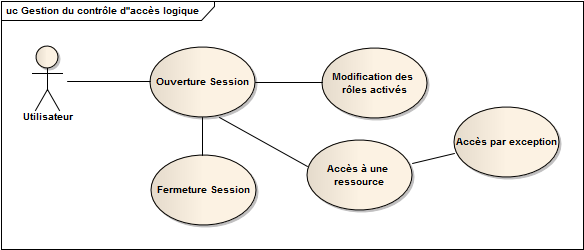


Figure 4 : Les scénarios de la gestion d'accès logique

* + - 1. Ouverture de session :

Lors de l'ouverture d'une session, le système :

1. Vérifie l'identité de l'utilisateur;
2. Vérifie que cet utilisateur est autorisé d'ouvrir une session sur le système;
3. Afficher à l'utilisateur les rôles qu'il est autorisé à activer (rôle dans le cadre d'une fonction ou une exception valide);
4. Ouvre une session et garde trace des actions de l'utilisateur;
5. Vérifie que les rôles demandés simultanément ne sont pas incompatibles.
   * + 1. Accès à une ressource :

Le système vérifie les droits accordés à l'utilisateur pour effectuer des opérations sur la ressource demandée.

Les autres scénarios sont détaillés en annexe (Voir annexe [7.3](#scen1)).

* + 1. Modalités d'administration des autorisations :
       1. Principe d'administration des autorisations :

Dans certains établissements de santé de grandes taille, le nombre de rôles est très important ce qui génère une grande charge d'administration. Cette administration consiste en :

- La description de l'organisation de l'établissement en éléments de structure;

- La définition des rôles et de leur hiérarchie;

- L'attribution d'autorisation aux rôles;

- L'affectation des utilisateurs aux éléments de structure avec un certain rôle.

Ces affectations de rôle peuvent être faites d'une façon centralisée (par un responsable) ou d'une façon décentralisée (locale par un ensemble de responsables).

* + - 1. Scénarios d'administration des autorisations :

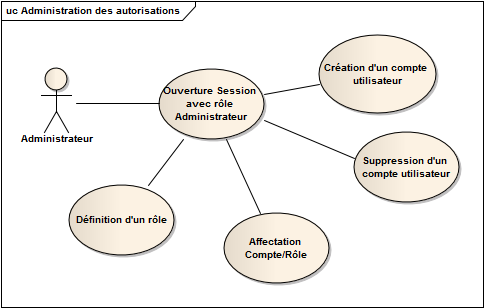


Figure 5 : Les scénarios de l'administration des autorisations

Les scénarios sont détaillés en annexe (Voir annexe [7.4](#scen2)).

* + - 1. Modèles d'organisation pour l'administration des autorisations :

Ci-après, on définit quelques principes sur lesquels on s'appuie lors de la mise en œuvre de la politique de sécurité :

* + - * 1. Définition des rôles :

Consiste à créer des rôles génériques représentant une activité et à leur attribuer les autorisations permettant d'exercer cette activité.

* + - * 1. Attribution des rôles aux utilisateurs :

Consiste à affecter un utilisateur à un élément de structure et lui attribuer un rôle dans cette structure. On détermine trois modèles d'organisation envisageables :

* + Modèle centralisé : dans ce modèle, les ressources humaines sont considérées comme une référence centrale pour l'administration des droits d'accès.
  + Modèle semi-décentralisé : ce modèle sollicite moins les ressources humaines et implique plus de personnes administratives. Une personne attribue les droits, et une autre personne les valide.
  + Modèle décentralisé : ce modèle implique fortement le personnel d'encadrement tout en évitant de compromettre le niveau de sécurité.
  1. Principes et règles de gestion
     1. Politique d’autorisation
        1. Principe général
  + Règle 1 « Politique d’autorisation »

La politique d’autorisation de l’établissement doit aboutir à la définition claire de règles de contrôle d’accès logique et à l’élaboration d’une liste de groupes d’utilisateurs et de leurs droits d’accès respectifs.

* + Règle 2 « Formalisation des responsabilités en matière de contrôles d’accès logique »

L’établissement prend toute mesure interne de nature à notifier au personnel le contenu de ses obligations en matière de contrôle d’accès logique (règlement intérieur, procédures internes).

* + Règle 3 « Charte d’utilisation des moyens informatiques »

L’établissement définit et diffuse à l’ensemble de ses utilisateurs une charte d’utilisation des moyens informatiques précisant les obligations de sécurité à respecter et reprenant les points essentiels de la politique d’autorisation :

- Quels sont les services et réseaux auxquels les utilisateurs ont accès.

- Quelle est la procédure permettant d’attribuer des droits d’accès à un utilisateur donné.

- Quelles sont les procédures de gestion et de contrôle des accès.

* + Règle 4 « Classification de ressources accédées »

Des autorisations d’accès adaptées à la classification des ressources accédées, doivent être mise en œuvre, exemple :

- Information publique : tout utilisateur authentifié peut accéder à ces informations.

- Information « accès restreint » : accès protégé par contrôle d’accès logique.

- Information « secret médical » ou « secret professionnel » : accès filtré selon les attributions précises de l’utilisateur (accès à tout ou partie du dossier …).

- Information « haute protection » : accès limité à quelques utilisateurs spécifiquement identifiés.

* + Règle 5 « Identification des caractéristiques de sécurité des services »

L’établissement réalise un catalogue des services informatiques et des services réseau disponible, et indique pour chacun d’entre eux les caractéristiques de sécurité qui leur sont propres :

- Fonctions de sécurité apportées.

- Besoin de sécurité du service.

* + Règle 6 « Contractualisation des exigences de contrôle d’accès logique »

L’établissement communique à ses prestataires et fournisseur un cahier des charges clair détaillant les fonctionnalités et exigences de sécurité attendues en matière de contrôle d’accès sur les systèmes dont ils ont la charge.

* + Règle 7 « Isolation des systèmes de haute sensibilité »

- La sensibilité de chaque application doit être évaluée et documentée explicitement, conformément à la politique d’autorisation.

- Lorsque, malgré sa haute sensibilité, une application doit fonctionner dans un environnement partagé, les autres applications avec lesquelles elle partage des ressources doivent être identifiées et fiable.

* + 1. Gestion du contrôle d’accès logique :
       1. Principe : Concepts élémentaires :
  + Règle 1 « Limitation des horaires de connexion »

L’établissement renforce le contrôle d’accès logique à son système d’information par des restrictions sur les horaires de connexion autorisés, généralement basé sur les horaires de travail du personnel concerné.

* + Règle 2 « Vérification du droit d’accès à un ressource »

L’accès effectif est accordé à l’utilisateur après vérification d’éléments de contexte complémentaires aux autorisations regroupé dans son ou ses rôles et qui sont spécifiés dans la partie 1 de la politique d’autorisation.

* + Règle 3 « Contrôle d’accès applicatif »
* Limiter l’accès aux fonctionnalités autorisées dans les menus présentés aux utilisateurs.
* Limiter les connaissances des utilisateurs sur les informations et fonctionnalités disponibles dans l'application à celle auxquelles ils sont autorisés à accéder.
* Limiter la documentation fournie aux utilisateurs à la présentation des fonctionnalités auxquelles ils ont accès.
  + Règle 4 « Mécanisme d’exception »

Un mécanisme de dérogation au contrôle d’accès logique doit permettre d’obtenir une autorisation d’accès exceptionnelle qui se fait selon un mécanisme déclaratif, indiquant le motif de l’exception, et précisant la durée accordée. Cette autorisation exceptionnelle fait l’objet de règles de journalisation spécifiques permettant un suivi détaillé des actions réalisées.

* + - 1. Principe : Mutualisation de l’infrastructure du contrôle d’accès logique
  + Règle 1 « Infrastructure de contrôle d’accès »

La gestion du contrôle d’accès devra être conforme au modèle retenu sur l’ensemble du système d’information, et elle est assurée de manière globale par un outil logiciel.

* + Règle 2 « Référentiel d’authentification des utilisateurs »

Les technologies disponibles permettant d’authentifier un utilisateur sont variées, tel que la saisie d’un mot de passe, la biométrie, l’utilisation de jetons matériels, d’une carte à puce ...

Les données d’identification contenues dans l’annuaire géré par le GIP CPS constituent la référence nationale pour l’authentification des professionnels de santé. L’établissement gère la cohérence entre les données d’identification gérées localement et l’annuaire du GIP CPS.

* + Règle 3 « Authentification des utilisateurs internes à l’établissement »

Dans tous les cas d’accès à des informations sensibles, et notamment à un DIS, l’établissement utilise des solutions d’authentification.

* + Règle 4 « Authentification des utilisateurs externes à l’établissement »

L’établissement utilise la carte de professionnel de santé comme moyen d’authentification des professionnels de santé n’exerçant pas en son sein.

* + - 1. Principe : Gestion des authentifiants

Si l’authentification lors de l’accès au système est réalisée sur la base d’un mot de passe, l’établissement s’assure que les règles suivantes sont respectées :

* + Règle 1 « Utilisation des authentifiants »

L’authentifiant d’un utilisateur est l’élément permettant de lui attribuer des droits d’accès, mais aussi de lui rendre responsable des actions réalisées sous son nom. Chaque utilisateur doit donc être informé que l’authentifiant est personnel et confidentiel, alors, il ne doit pas le prêter à un tiers, ni s’authentifier pour laisser un tiers utiliser ses droits.

* + Règle 2 « Gestion des mots de passe par les utilisateurs »
* Les procédures internes informent chaque utilisateur qu’il est responsable de l’utilisation de ses mots de passe, il ne doit pas les divulguer.
* Lorsque les utilisateurs sont chargés de maintenir eux-mêmes leurs propres mots de passe, un mot de passe temporaire doit leur être attribué, et ils devront le changer immédiatement.
* Si un utilisateur a oublié son mot de passe, un mot de passe temporaire doit lui être généré après identification certaine de l’utilisateur.
* La transmission des mots de passe temporaire doit être sûre, et ne doit pas être réalisée en clair via un tiers ou via une messagerie électronique non protégée.
* L’utilisateur doit accuser réception de ses mots de passe.
  + Règle 3 « Sécurité de la saisie des mots de passe »
* La saisie d’un nouveau mot de passe doit faire l’objet d’une double saisie (1ère saisie + confirmation) pour éviter les erreurs de frappe.
* Ne pas afficher les mots de passes lors de leur saisie.
  + Règle 4 « Qualité des mots de passe »
* Longueur minimale du mot de passe (8 caractères recommandés pour les utilisateurs, 14 pour les administrateurs) en utilisant à la fois des chiffres et des lettres (minuscules et majuscules).
* Mémorisation facile (proposer des procédés mnémotechnique tels que les anagrammes).
* Pas de répétition consécutive d’un même caractère ou groupe de caractère (ex : abccccd…).
  + Règle 5 « Stockage des mots de passe »

- Stocker les mots de passe dans des fichiers séparés des données applicatives.

- Stocker les mots de passe sous une forme chiffrée à l’aide d’un algorithme à sens unique.

- Changer tous les mots de passe définis par défaut par le fournisseur ou l’installeur d’un nouveau système.

* + Règle 6 « Protection de la confidentialité des mots de passe »

Eviter d’écrire les mots de passe sur un papier. Si c’est absolument indispensable, conserver celui-ci dans un endroit sûr.

- Changer le mot de passe s’il y a la moindre possibilité sue celui-ci soit connu d’un tiers.

- Ne pas construire ses mots de passe sur la base d’informations que l’on peut facilement deviner si l’on connaît l’utilisateur (nom, prénom, …..).

- Changer les mots de passe temporaires dès la 1ère connexion.

- Changer les mots de passe régulièrement, et ne pas réutiliser un ancien mot de passe.

* + - 1. Principe : Ouverture d’une session :
  + Règle 1 « Procédure de connexion au poste de travail »

Afin de limiter les accès non autorisés, l’établissement met en place un processus sûr de connexion aux postes de travail qui consiste à :

- Afficher une mention précisant que l’accès au système est réservé aux utilisateurs autorisés.

- Ne fournir aucun message susceptible d’aider un utilisateur non autorisé.

- Ne valider la connexion qu’une fois fournies toutes les informations nécessaires à l’authentification. En cas d’erreur, le message d’erreur ne doit pas indiquer la nature.

- Limiter le nombre de tentatives infructueuses permises, et imposer un délai avant que de nouvelles tentatives ne puissent être effectuées.

- Journaliser toutes les tentatives infructueuses.

- Limiter le délai autorisé pour effectuer le processus complet d’ouverture de session, et interrompre ce processus en cas de dépassement de délai.

- Afficher la date et l’heure de la dernière connexion réussie ainsi que le détail des tentatives infructueuses survenues depuis, à chaque ouverture de session.

* + Règle 2 « Clôture de session »

- Une procédure permettant de clôturer les sessions et générant une trace de clôture, est définie.

- Les sessions inactives au-delà d’une durée déterminée par l’établissement doivent être automatiquement fermées.

* + 1. Traçabilité des accès :
       1. Principe : Génération des traces dans l’administration des autorisations :

La traçabilité des accès permet d’être au courant des autorisations d’un utilisateur à un moment donné, Quels utilisateurs avaient accès à un élément de dossier et dans quelles conditions, ainsi de savoir qui a créé, modifié ou supprimer des droits et quand.

* + Règle 1 « Journalisation des évènements »

Afin de structurer la surveillance du contrôle d’accès logique et faciliter les enquêtes futures, l’établissement tient des journaux d’audit où sont enregistrées les anomalies, exception et autres évènements relatifs à la sécurité.

* + Règle 2 « Contenu des journaux d’audit »
* L’identifiant des utilisateurs.
* Les dates et heures d’ouverture de sessions.
* La date et l’heure de l’événement.
* L’identité du terminal utilisé si c’est possible.
* Les références aux informations accédées et aux traitements réalisés ainsi que leurs résultats.
* La description de l’opération ou de l’événement journalisé.
  + Règle 3 « Possibilité d’interrogation des journaux »

Les traces de mise à jour des habilitations doivent être restituées selon plusieurs critères tels que la date, l’origine de la mise à jour, l’utilisateur concerné …

* + Règle 4 « Archivage des traces »

Les journaux d’audit doivent être archivés pendant une durée de conservation des informations accédées définit au préalable par l’établissement. Cet archivage va fournir des preuves en cas de litige.

* + Règle 5 « Synchronisation des horloges »

L’établissement met en place une procédure organisationnelle assurant la synchronisation des horloges de ses systèmes qui sont utilisées comme références horaires dans les journaux d’audit, susceptible d’être utilisée comme élément de preuve pour les enquêtes.

* + - 1. Principe : Traçabilité en accès exceptionnel
  + Règle 1 « Renforcement de la journalisation dans l’utilisation des mécanismes d’exception »

Il est indispensable de tracer la totalité des actions réalisées grâce au mécanisme d’exception dans des journaux spécifiques.

* + Règle 2 « Nettoyage des journaux d’exception »

Le responsable de la supervision du mécanisme d’exception doit confirmer la légitimité de la justification de cette exception, fournie par l’utilisateur et qui doit être journalisée.

Suite à cette confirmation, les traces renforcées sont supprimées.

* + 1. Administration des autorisations et supervision du contrôle d’accès
       1. Principe : Gestion des droits par rôles génériques
  + Règle 1 « Utilisation des rôles correspondant à des métiers ou à des missions »

Une liste de rôles est attribuée à chaque utilisateur, dont chaque rôle regroupe des autorisations reflétant une mission ou un métier spécifique.

* + Règle 2 « Rôles obligatoires »

Trois rôles doivent être définis au minimum pour chaque application : utilisateur, superviseur et paramétrage.

* + Règle 3 « Séparation des pouvoirs dans les rôles »

Les rôles doivent être définis de telle manière qu’il soit impossible au personnel non opérationnel d’accéder aux données de production en mise à jour.

* + - 1. Principe : Définition des rôles
  + Règle 1 « Responsabilité de la définition des rôles »

La définition des rôles doit être prévue par le responsable de la ressource et validée par le collège d’information médicale.

* + Règle 2 « Principe de moindre privilège »

Un utilisateur ne doit pas disposer de plus de droits que ne l’exigent ses activités réelles.

* + Règle 3 « Documentation de la définition des rôles »

La définition des rôles doit être regroupée dans un document validé par la direction de l’établissement et diffusé à l’administration des autorisations.

* + Règle 4 « Contrôle renforcé sur l’accès aux fonctions privilégiées »
* Encourager l’utilisation de routines systèmes pour éviter au maximum la nécessité d’accorder ces autorisations privilégiées aux utilisateurs.
* Attribuer ces autorisations privilégiées ans des rôles différents de ceux utilisés par les utilisateurs pour leur activités courantes.
  + Règle 5 « Restriction de l’accès aux utilitaires système »

Certains systèmes utilitaires permettent de contourner le contrôle d’accès logique du système d’exploitation ou des applications. L’accès à ces utilitaires doit respecter la règle précédente, et en complément :

* Authentification préalable avant l’accès à l’utilitaire (en plus de l’authentification par défaut)
* Séparation des utilitaires systèmes et des applications.
* Stricte limitation de l’accès aux utilitaires aux utilisateurs autorisés et confidents.
* Journalisation spécifique de l’utilisation de ces utilitaires.
* Définition et documentation des rôles spécifiques et des niveaux d’autorisations nécessaires pour l’accès à ces utilitaires.
* Suppression après l’installation de tous les utilitaires et logiciels systèmes inutiles.
  + - 1. Principe : Création des comptes des utilisateurs
  + Règle 1 « Procédures d’enregistrement des utilisateurs »

L’établissement définit et diffuse des procédures permettant l’enregistrement initial des utilisateurs, ainsi que la révocation définitive de leurs droits.

* + Règle 2 « Identification unique des utilisateurs »

Chaque utilisateur dispose d’un identifiant unique, qui permet de l’identifier sans ambiguïté.

* + Règle 3 « Enregistrement des utilisateurs internes »

Chaque utilisateur interne dispose d’un compte unique, qui lui est créé lors de son recrutement.

* + Règle 4 « Enregistrement des utilisateurs externes »

Chaque utilisateur externe dispose d’un compte unique. La signature d’une convention définissant les engagements réciproques de l’établissement et de l’utilisateur externe est indispensable.

* + Règle 5 « Enregistrement des patients »

Dans le cas d’un établissement où le patient doit pouvoir consulter et mettre à jour son dossier électronique, un compte lui permettant d’accéder au SIS lui sera donc ouvert, sur sa demande.

* + Règle 6 « Caractère transactionnel de la procédure d’enregistrement des utilisateurs »

Aucun droit n’est accordé à l’utilisateur tant que cette procédure n’est pas terminée.

* + Règle 7 « Référentiel des utilisateurs »
* Un référentiel de tous les utilisateurs enregistrés avec leurs différents droits d’accès.
* Un référentiel des patients.
  + - 1. Principe : Attribution de droits aux utilisateurs
  + Règle 1 « Responsabilités des utilisateurs »
* Remise aux utilisateurs d’un document écrit contenant leurs droits et leurs responsabilités.
* Signature par l’utilisateur d’un récépissé confirmant que celui-ci comprend et accepte ces droits et devoirs.
  + Règle 2 « Restriction des possibilités d’attribution de rôles »

Un utilisateur ne doit pouvoir attribuer que les rôles correspondant aux activités des utilisateurs qu’il encadre.

* + Règle 3 « Possibilités de délégation de l’attribution de rôles »

Un utilisateur doit pouvoir déléguer ses propres droits d’administration à l’un de ses collaborateurs.

* + - 1. Principe : Mise à jour et révocation des droits des utilisateurs
  + Règle 1 « Mise à jour des droits des utilisateurs »

Permettre la mise à jour, dans les plus brefs délais, des autorisations des utilisateurs ayant changé de fonction.

* + Règle 2 « Révocation des droits des utilisateurs en cas de départ définitif »

La désactivation, dans les plus brefs délais, du compte d’utilisateurs ayant quitté l’établissement.

* + Règle 3 « Suspension des droits des utilisateurs temporairement absents »

Le compte de tout utilisateur quittant l’établissement temporairement, doit être désactivé dans les plus brefs délais.

* + - 1. Principe : Règles de supervision du contrôle d’accès
  + Règle 1 « Audit périodique du registre des utilisateurs »

La vérification périodique du registre des utilisateurs pour s’assurer que les rôles qui leur sont attribués correspondent à leurs fonctions, ainsi que la révocation des autorisations correspondent aux comptes non utilisés.

* + Règle 2 « Revues des rôles »
* Revues des rôles utilisateurs tous les 6 mois et après chaque évolution significative d’un système d’information.
* Revue des rôles disposant de droits privilégiés (administrateur) tous les 3 mois.
  + Règle 3 « Information élémentaires pour le suivi des risques »

La mise en œuvre de procédures de surveillance des aspects suivants :

* Suivi des accès.
* Accès aux opérations privilégiées.
* Tentatives d’accès non autorisées.
* Alertes ou défaillances des systèmes.
  + Règle 4 « Indicateurs de risque sur les systèmes et réseaux »

L’établissement examine régulièrement les journaux de sécurité en respectant le principe de séparation des pouvoirs (l’auditeur est différent de la personne auditée).

* + Règle 5 « Surveillance des outils de journalisation »

Surveiller l’activation et la désactivation des outils de journalisation, les modifications et les suppressions, l’épuisement des supports de stockage des journaux … etc.

* 1. Conclusion

Le développement et la mise en œuvre d’une politique d’autorisation demeure une étape primordiale dans le processus de maîtrise des risques. La mise en place des principes de gestion des autorisations adaptées aux fortes contraintes des systèmes d’information médicaux sera en effet un passage obligé pour atteindre des objectifs élevés de confidentialité des données personnelles de santé.

1. Autoévaluation :
   1. Introduction :

Dans le cadre de déterminer la politique appropriée à un établissement de santé particulier on aboutit à l’utilisation d’un guide d’auto-évaluation qui permet de déterminer le niveau de sécurité actuel et propose une politique de sécurité convient au cas de l’établissement.

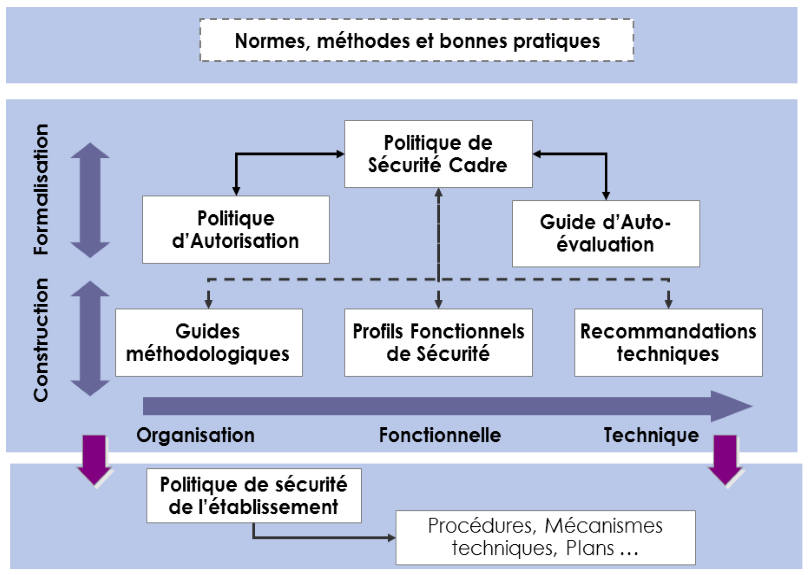


Figure 7 : le positionnement de l’auto-évaluation par rapport à la politique de la sécurité cadre

* 1. Définition de l’auto-évaluation :

L’auto-évaluation, pour un établissement de santé, est de se situer par-rapport à la PSC-SI (politique de sécurité cadre) et leur risques spécifiques

Le guide d’auto-évaluation est constitué d’un support logiciel et d’un manuel d’utilisation permettant de guider l’établissement dans son évaluation et l’élaboration d’un plan de sécurité pluriannuel.

* + 1. Les objectifs d’un guide d’auto-évaluation :
* Apprécier le degré de Maturité en termes de sécurité de l’information par rapport aux règles établies par la PSC-SI ;
* Identifier son niveau de risque en fonction des résultats obtenus et de menaces pesant sur le system d’information ;
* Identifier les actions prioritaires à conduire à fin de minimiser les risques identifiés ;
* Construire un plan d’action pluriannuel afin de mettre en œuvre la politique de sécurité ;
  + 1. Cycle de vie de l’auto-évaluation d’un établissement :

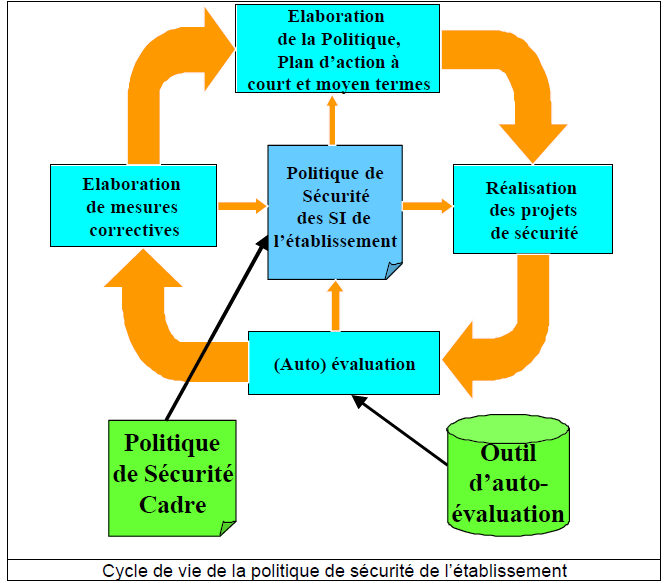


Figure 8 : Cycle de vie de la politique de sécurité de l’établissement

* + Commentaires :

L’auto-évaluation du niveau de sécurité de l’établissement : cette autoévaluation permet de :

* Faire un état des lieux de la sécurité des systèmes d’information de l’établissement (Mesure de sa conformité par rapport principes de la politique de sécurité cadre) ;
* Etablir un plan d’action sécurité comprenant des actions à court terme pour supprimer d’urgence des vulnérabilités importantes, et des projets à moyen terme pour construire une politique de sécurité cohérente et efficace ;
* Réaliser des actions court terme ;
* Rédiger la politique de sécurité de l’établissement ;
* Réaliser des projets à moyen terme ;
* S’évaluer suite à la réalisation du plan d’action et élaborer les mesures correctives à la Politique de sécurité de l’établissement ;
  1. Présentation du guide d’auto-évaluation :

C’est un support bureautique conçu par la GMSIH. Il permet aux établissements de santé d’auto-évaluer le niveau de Sécurité de leurs Systèmes d’Information (SSI).

Il a été conçu pour faciliter la tâche d’auto-évaluation en basant sur deux idées maîtresses :

* L’obtention rapide de résultats cohérents et « parlants » ;
* La facilité d’emploi et l’ergonomie du support pour l’utilisateur.

La mission de l’évaluateur consiste à remplir un questionnaire de 100 questions en choisissant les réponses les plus appropriées correspondant à son environnement.

Le support réalise de façon automatique :

* La présentation des résultats de l’évaluation (positionner l’état actuel de la sécurité par rapport à la PSC-SI) ;
* Une aide à la construction d’un plan d’action ;
  + 1. Fonctionnement du logiciel :
       1. Questionnaire d’auto-évaluation  (étape d’évaluation):

C’est un questionnaire de 100 questions dont les thématiques sont:

* + Politique de sécurité
  + Management de la sécurité
  + Inventaire et classification des ressources
  + Sécurité et ressources humaines
  + Sécurité physique et sécurité de l’environnement
  + Exploitation informatique et gestion des réseaux
  + Contrôle d’accès logique
  + Développement et maintenance des applications et des systèmes
  + Gestion de la continuité
  + Respect de la réglementation interne et externe

Le but de ce questionnaire est d’établir un état de lieu pour évaluer le dégrées de risque actuel, pour cela on affecte un coefficient de pondération à chaque repense et on obtiendra à la fin une note représente le degré de risque qui est la moyenne pondérée par principes des notes obtenues.

À la fin du traitement on obtient un score entre 0 et 4 représente la maturité des principes de l’établissement (plus la note est élevée plus la maturité est importante).

* + - 1. L’état du lieu :

A partir des résultats obtenus dans l’étape d’évaluation, le logiciel représente l’état de lieu graphiquement en comparant la moyenne de degré de maturité avec le niveau de maturité considéré par le GMSIH comme satisfaisant en matière de sécurité : Niveau 3 et positionne le niveau de maturité par principe.

Les résultats sont présentés en rosace de la maturité des principes de l’établissement.

Plus les branches de la rosace (principe) sont éloignées du centre, plus laMaturité est proche de l’excellence.

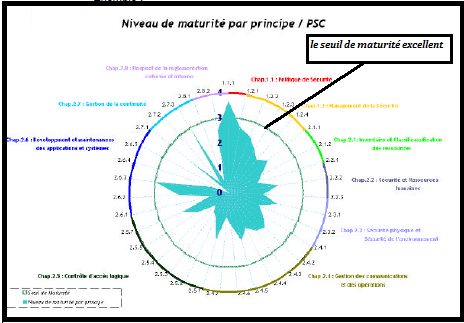


Figure 9 : Rosace de la maturité des principes de l’établissement

* + - 1. Le degré de couverture :

A partir du :

* + Seuil de maturité des principes de l’établissement ;
  + Une table de menace prédéfinie ;
  + Une table technique permettant de considérer la contribution en matière de réduction de risque ;
  + Une table d’aversion au risque.

Le logiciel calcule la gravité (impact et potentialité de survenance) de chaque menace sur l’établissement et représente les résultats sur une rosace de gravité (Plus l’aire de la rosace est grande plus le risque lié à la menace est Important)

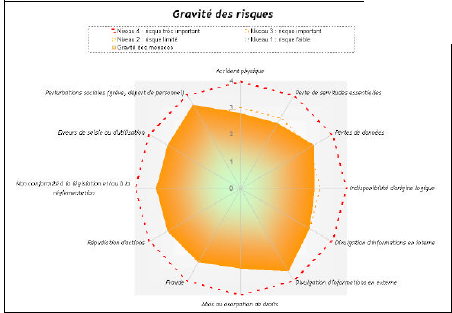


Figure 10 : Rosace de gravité

* + Traduction:
* Lorsque l’aire atteint le niveau 1 ou 2, le risque est tolérable.
* Lorsque l’aire atteint le niveau 3, le risque est important. Des mesures doivent être prises pour le réduire.
* Lorsque l’aire atteint le niveau 4, le risque est très important. Des mesures urgentes doivent être prises.

Les menaces de niveau 3 et 4 sont entre autres réellement pertinentes ; les risques liés à ces menaces en termes d’impact et/ou de potentialité sont très importants pour l’Etablissement.

La grille suivante représente le degré du risque en fonction des repenses :

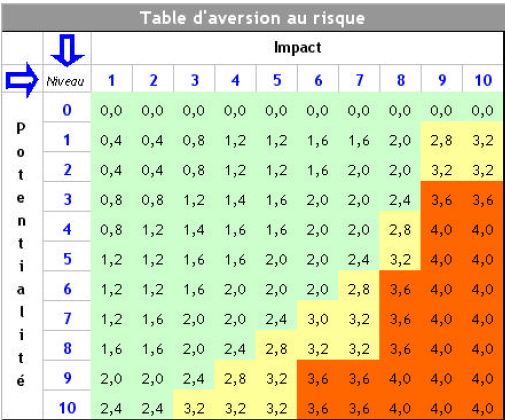


Figure 11 : Grille de degré du risque en fonction des repenses

* + Explications:
* La mesure globale du risque ne résulte pas d’une opération mathématique, mais d’une estimation de sa Gravité. Cette importance du risque peut être traduite sur une grille matricielle à deux entrées :
  + - L’impact (ou la perte pour l’organisme) ;
    - La potentialité (ou la probabilité de survenance) ;
* La table d’aversion au risque définit en fonction des niveaux (de 1 à 10) ***l’impact*** et ***la potentialité*** estimés, si le risque est acceptable ou pas (Gravité). Ainsi dans cette table :
  + - Une Gravité du risque [3,5 ; 4] correspond à un risque inacceptable qui devrait faire l’objet de mesures urgentes ;
    - Une Gravité du risque [2,5 ; 3,4] correspond à un risque inadmissible qui devrait être réduit à échéance déterminée ;
    - Une Gravité du risque [0,0 ; 2,4] correspond à un risque toléré urgentes[.[3]](#AutoEval)
      * 1. Table de menace prédéfinie :

|  |  |
| --- | --- |
| Menace | Définition |
| Accident physique | Les accidents physiques recouvrent toutes les menaces de type « destruction de matériel suite à un accident » :   * + incendie ;   + dégâts des eaux (inondations, ruptures de canalisations…) ;   + foudre ;   + tempête |
| Perte de servitudes essentielles | ce sont les menaces essentielles sont les menaces correspondant à l’indisponibilité temporaire ou permanente d’un service indispensable au fonctionnement du système d’information, mais dont la fourniture ne dépend pas de l’établissement :   * + perte d’alimentation électrique ;   + perte d’alimentation en eau (pour certaines installations de climatisation) ;   + défaillance de l’opérateur de télécommunications ; |
| Perte de données | Les pertes de données correspondent à l’indisponibilité de données définitive (et non volontaire), suite par exemple à une destruction physique de matériel, mais aussi suite à l’effacement ou la corruption définitifs de ces données, qu’il soit accidentel ou malveillant :   * + crash disque (sans sauvegardes) ;   + effacement involontaire d’un fichier ;   + altération de support amovible ; |
| Indisponibilité d’origine logique | L’indisponibilité d’origine logique est l’impossibilité d’accéder à des services ou à des informations suite à une défaillance non matérielle ou un manque de performance du système d’information l’amenant à un niveau de disponibilité insuffisant sous-dimensionnement des systèmes et des réseaux :   * + insuffisance de puissance processeur,   + engorgement des disques,   + saturation de la mémoire,   + engorgement du réseau ou d’un élément du réseau ;   + attaques en déni de service ; |
| Divulgation d’informations en interne | La divulgation d’information en interne correspond au fait qu’un personnel de l’établissement prenne connaissance d’une information pour laquelle il n’est normalement pas habilité, que ce soit volontairement ou non :   * + accès à un dossier patient par un personnel de l’établissement non habilité ; |
| Divulgation d’informations en externe | La divulgation d’information en externe correspond au fait qu’un tiers à l’établissement prenne connaissance d’une information pour laquelle il n’est normalement pas habilité, que ce soit volontairement ou non :   * + accès à un dossier patient par un visiteur ; |
| Abus ou usurpation de droits | L’abus ou l’usurpation de droits consiste à outrepasser ses droits d’accès ou à utiliser les droits d’un tiers (en usurpant son identité ou non) pour réaliser des opérations ou accéder à des informations sans y être habilité :   * + utilisation du login/authentifiant de quelqu’un d’autre pour accéder à des ressources ou des informations non autorisées ; |
| Fraude | La fraude consiste à mener des actions illicites et déloyales dans un but d’enrichissement personnel :   * + détournement de fonds ;   + détournement de matériels ;   + vol de médicaments ;   + recel d’informations |
| Reniement d’actions | Le reniement d’actions consiste à nier être l’auteur d’actions qui vous sont imputées. |
| Non-conformité à la législation | personnel, de ne pas respecter le cadre juridique et réglementaire concernant les activités, qu’il s’agisse du cadre lié à la santé et aux systèmes d’information de santé ou du cadre lié à l’informatique en général :   * + confidentialité du dossier patient ;   + droits du patient ;   + respect de la vie privée (surveillance…) ; |
| Erreurs de saisie ou d’utilisation | Les erreurs de saisie ou d’utilisation consistent à, involontairement :   * + saisir dans le système d’information des informations erronées ;   + mal interpréter des informations restituées par le système ;   + mal utiliser ses fonctionnalités. |
| Perturbation sociale | Les perturbations sociales correspondent d’une part aux grèves ou au personnel suite à des incidents informatiques ou à l’utilisation des systèmes d’information ; d’autre part à toute autre perturbation sociale ayant une conséquence sur le fonctionnement des systèmes d’information :   * + grève de personnel stratégique (ex. : administrateurs systèmes),   + grève avec « prise en otage » des systèmes informatiques… |

Tableau 4 : Table de menaces prédéfinies

* + - 1. Efficacité des principes (classification des principes par priorité):

A partir du degré de maturité des principes de l’établissement et du degré de gravité de chaque menace pour l’établissement et d’un coefficient d’orientation (**1** ou **4**) permettant de mettre en valeur des principes de sécurité dont la mise en œuvre est fondamentale pour les Etablissements de Santé, le logiciel calcule le besoin d’amélioration (efficacité) de chaque principe en matière de couverture des risques inhérents à l’établissement.

Les résultats sont représentés en un diagramme à barre de l’efficacité des principes de sécurité en termes de réductions des risques liés à l’établissement.

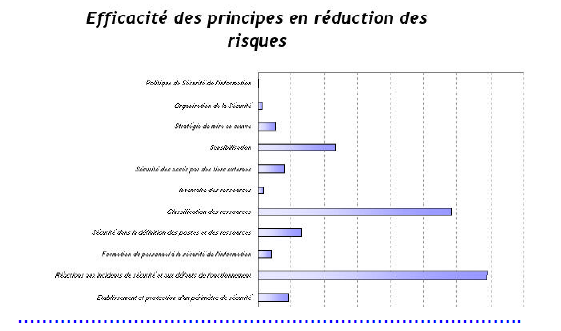


Figure 12 : Diagramme de l’efficacité des principes de sécurité en réductions des risques

* + - 1. Priorités d’action :

A partir de l’efficacité de chaque principe en matière de couverture des risques pour l’Etablissement, le logiciel calcule pour chaque principe une note d’efficacité puis il trie ces principes en ordre décroissant (les principes les plus contributifs à la sécurité et qui seraient à mettre en œuvre en priorité sont classés les premiers) le logiciel affiche les résultats sous forme d’une liste.

* + Exemple :



Figure 13 : Liste des principes ordonnés selon la priorité

* + - 1. Ordonnancement :

A partir de la liste des principes ordonnés selon leur efficacité croissante en matière de réduction des risques et le schéma d’ordonnancement théorique des dépendances fonctionnelles. Ce schéma est issu des notions de « pré requis » et «préalable à » caractérisant les principes de la **P**olitique de **S**écurité **C**adre, le logiciel effectue l’ordonnancement des principes entre eux en fonction :

* + - De leur priorité effective ;
    - De leur ordonnancement théorique.

1. Conclusion :

La mise en œuvre d'une politique de sécurité est un projet qui requiert la collaboration de tout le personnel et les membres de la direction de l'établissement de santé puisqu'elle représente un élément essentiel pour instaurer un climat de confiance qui favorise l'échange et le partage de données de santé à caractère personnel. Toutefois, l'état du SIH de l'établissement consiste le facteur majeur dans la réussite et la longue-tenue de cette politique, puisqu'il en représente la base. Il faut veillez aussi à mettre à jour la politique de sécurité du SIH périodiquement car les risques liés au domaine hospitalier sont en croissance qui peut être imprédictible.

1. Glossaire

**DIS (Domaine d’information de santé) :** c’est un ensemble constitué des données de santé à caractère personnel produites par les professionnels de santé d’une structure participant à la prévention et au soin, conservées sous leur responsabilité et organisées en un système d’information.

**Professionnel de santé (PS)** : Ce terme regroupe entre outre les médecins, infirmières, techniciens médicaux, auxiliaires de soins, pharmaciens, laborantins, ainsi que d’autres utilisateurs et organismes.

1. Annexe :
   1. Règles du principe :

|  |  |  |
| --- | --- | --- |
| Chapitre 1 : Politique de sécurité | | |
| Principe 1.1 Politique de sécurité de l’information | « Doter l’établissement d’une politique de sécurité de l’information publiée et soutenue par la Direction » | Politique de sécurité |
| Règle 1.1.1 Elaboration et publication du document de Politique de Sécurité de  l’Information de l’établissement | | |
| Règle 1.1.2 Suivi de la politique de sécurité de l’information | | |

|  |  |  |
| --- | --- | --- |
| Chapitre 2 : Management de la sécurité | | |
| Principe 2.1 Organisation de la sécurité | « Gérer la sécurité de l’information au sein de l’organisation de santé » | Infrastructure de la sécurité de l’information |
| Règle 2.1.1 Attribution des responsabilités de la sécurité du système d’information | | |
| Règle 2.1.2 Comité de sécurité du système d’information (niveau décisionnel) | | |
| Règle 2.1.3 Nomination d’un RSSI avec délégation formelle du Directeur | | |
| Règle 2.1.4 Comité opérationnel de sécurité du système d’information | | |
| Règle 2.1.5 Intégration des nouvelles configurations et applications | | |
| Règle 2.1.6 Recours à des experts et développement de la coopération entre  Organisations | | |
| Règle 2.1.7 Examen indépendant de l’application de la politique de sécurité | | |
| Principe 2.2 Stratégie de mise en œuvre | « Garantir par application d’une démarche de sécurité pour le système d’information de l’établissement que :   1. Les exigences de sécurité sont bien déterminées après une évaluation des risques. 2. Les mesures prises pour remplir les exigences de sécurité sont bien proportionnelles au risque encouru. » | / |
| Règle 2.2.1 Première étape : prendre conscience du besoin de sécurité pour les systèmes d’information et procéder à l’autoévaluation de la sécurité du système d’information | | |
| Règle 2.2.2 Deuxième étape : établir le plan d’actions sécurité | | |
| Règle 2.2.3 Evaluation périodique des risques X | | |
| Règle 2.2.4 Choix des mesures et démarrage des actions | | |
| Principe 2.3 Sensibilisation | 1. « Sensibiliser le personnel de l’établissement aux enjeux de la sécurité » 2. « Informer le personnel quant à sa responsabilité en matière de respect de la politique de sécurité » | / |
| Règle 2.3.1 Sensibilisation du personnel de l’établissement | | |
| Règle 2.3.2 Rôle du management dans la sensibilisation et la responsabilisation du  Personnel | | |
| Principe 2.4 Sécurité des interventions par des tiers externes | 1. « Maintenir la sécurité des infrastructures de traitement de l’information et des informations auxquelles des tiers ont accès» 2. « Maintenir la sécurité de l’information lorsque la responsabilité du traitement de l’information a été confiée à une autre organisation extérieure (sous-traitance)» | 1. Sécurité des accès par des tiers 2. Sous-traitance |
| Règle 2.4.1 Identification des risques relatifs aux types d’accès par des tiers externes | | |
| Règle 2.4.2 Identification des risques liés aux motifs d’accès par des tiers externes,  autres que dans le cadre d’une coopération à finalité de soins | | |
| Règle 2.4.3 Identification des risques liés à l’accès par des tiers dans le cadre d’une  coopération de soins (réseaux de santé, accès patient,…) | | |
| Règle 2.4.4 Exigences de sécurité dans les contrats de tiers, y compris dans les contrats  des réseaux de santé et dans la relation avec les patients | | |
| Règle 2.4.5 Mise en place de mesures de contrôle d’accès adaptées et leur intégration à  la politique d’autorisation pour les accès logiques des tiers, de participants à des réseaux  de santé, de patients | | |
| Règle 2.4.6 Exigences de sécurité dans les contrats de sous-traitance | | |

|  |  |  |
| --- | --- | --- |
| Chapitre 3 : Inventaire et classification des ressources | | |
| Principe 3.1 Inventaire des ressources | « Établir la liste des ressources nécessitant des mesures de protection appropriées » | Classification et contrôle des actifs |
| Règle 3.1.1 Inventaire des ressources | | |
| Règle 3.1.2 Identification du responsable des ressources | | |
| Principe 3.2 Classification des ressources | « Attribuer le niveau de protection requis pour chaque ressource du système  d’information » | / |
| Règle 3.2.1 Lignes directrices pour la classification des ressources | | |
| Règle 3.2.2 Responsabilité de la classification des ressources | | |
| Règle 3.2.3 Mise à jour de la classification des ressources | | |
| Règle 3.2.4 Étiquetage des ressources | | |
| Règle 3.2.5 Procédures de manipulation des ressources | | |

|  |  |  |
| --- | --- | --- |
| Chapitre 4 Sécurité et Ressources humaines | | |
| Principe 4.1 Sécurité dans la définition des postes et des ressources | « Établir la liste des ressources nécessitant des mesures de protection appropriées » | Sécurité dans la définition des postes et des ressources |
| Règle 4.1.1 La sécurité dans la définition des fiches de postes | | |
| Règle 4.1.2 Politique de recrutement | | |
| Règle 4.1.3 Respect du secret professionnel | | |
| Principe 4.2 Formation du personnel à la sécurité de l’information | « Soutenir la politique de sécurité des infrastructures et des informations »  « Aboutir à une efficacité opérationnelle dans l’utilisation des outils de  sécurité » | Formation des utilisateurs |
| Règle 4.2.1 Formation à la sécurité | | |
| Principe 4.3 Réactions aux incidents de sécurité et aux défauts de fonctionnement | « Permettre une information et une réaction rapide lors de constats d’incidents,  dysfonctionnements et failles de sécurité » | Réaction aux incidents de sécurité et aux défauts de fonctionnement |
| Règle 4.3.1 Signalement des incidents de sécurité | | |
| Règle 4.3.2 Signalement des failles de sécurité | | |
| Règle 4.3.3 Signalement du fonctionnement défectueux de logiciels | | |
| Règle 4.3.4 Suivi des incidents et des failles de sécurité | | |

|  |  |  |
| --- | --- | --- |
| Chapitre 5 Sécurité physique et sécurité de l’environnement | | |
| Principe 5.1 Etablissement et protection d’un périmètre de sécurité | 1. « Protéger les locaux et les informations de l’établissement des accès non autorisés (infractions) par les mesures adéquates » 2. « Protéger les locaux et les informations des dommages et des perturbations potentiels (accidents) par les mesures adéquates » 3. « Adapter la protection des zones de sécurité en fonction des risques particuliers à ces zones » 4. « Assurer l’adéquation entre les mesures de sécurité mises en œuvre dans le cadre de la Sécurité physique et les conditions du travail dans les zones de sécurité » 5. « Assurer un contrôle d’entrée et de sortie du périmètre de sécurité de l’établissement » | Zones de sécurité |
| Règle 5.1.1 Découpage du périmètre sensible et détermination des zones de sécurité  Physique | | |
| Règle 5.1.2 Protection des zones du périmètre de sécurité physique | | |
| Règle 5.1.3 Travail dans les zones de sécurité | | |
| Règle 5.1.4 Cloisonnement des zones de livraison et de chargement | | |
| Principe 5.2 Protection et sécurité du matériel | 1. « Empêcher toutes pertes, dommages ou compromissions de matériels et d’infrastructures nécessaires au bon fonctionnement de l’établissement en interne et en externe.» 2. « Eviter toute interruption des activités de l’établissement (matériel et alimentation) » 3. « Protéger physiquement le matériel de l’établissement contre les menaces d’atteinte à la sécurité et/ou les dangers liés à l’environnement ou à leur utilisation » | Sécurité du matériel |
| Règle 5.2.1 Localisation et utilisation du matériel informatique | | |
| Règle 5.2.2 Sécurité de l’alimentation électrique | | |
| Règle 5.2.3 Sécurité du câblage | | |
| Règle 5.2.4 Sécurité et maintenance du matériel | | |
| Règle 5.2.5 Sécurité du matériel utilisé à l’extérieur de l’établissement | | |
| Règle 5.2.6 Sécurité et mise au rebut ou réutilisation de matériel | | |
| Principe 5.3 Sécurité générale des matériels | « Empêcher la compromission ou le vol des informations et des infrastructures de traitement de l’information de l ‘établissement » | Mesures de contrôle générales |
| Règle 5.3.1 Sécurité du lieu et des outils de travail | | |
| Règle 5.3.2 Enlèvement des biens | | |

|  |  |  |
| --- | --- | --- |
| Chapitre 6 Exploitation informatique et gestion des réseaux | | |
| Principe 6.1 Procédures d’exploitation et responsabilités | « S’assurer de la fiabilité et de la sécurité des infrastructures de traitement de l’information et de leur exploitation » | Procédures et responsabilités opérationnelles |
| Règle 6.1.1 Documentation d’exploitation | | |
| Règle 6.1.2 Maintien à jour formel de la documentation d’exploitation | | |
| Règle 6.1.3 Maîtrise des modifications | | |
| Règle 6.1.4 Procédures de réaction sur incident | | |
| Règle 6.1.5 Séparation des responsabilités | | |
| Règle 6.1.6 Lutte contre la fraude | | |
| Règle 6.1.7 Indépendance de l’audit | | |
| Règle 6.1.8 Externalisation de la gestion des infrastructures (infogérance) | | |
| Principe 6.2 « Planification de la capacité » et recettes pour mise en exploitation | « Minimiser les risques de défaillance ou de surcharge des systèmes » | Planification et recette des systèmes |
| Règle 6.2.1 Planification de la capacité | | |
| Règle 6.2.2 Surveillance des serveurs centraux | | |
| Règle 6.2.3 Surveillance du parc bureautique et des postes de travail | | |
| Règle 6.6 Recette des systèmes | | |
| Principe 6.3 Protection contre les logiciels pernicieux | « Protéger l’intégrité des logiciels et de l’information » | Protection contre les logiciels pernicieux |
| Règle 6.3.1 Organisation de la lutte contre les logiciels pernicieux (ou lutte anti-virale) X | | |
| Règle 6.3.2 Usage des ressources informatiques | | |
| Règle 6.3.3 Dispositif de lutte anti –virale | | |
| Règle 6.3.4 Dispositif de lutte contre les codes pernicieux pour les supports externes et  la messagerie | | |
| Règle 6.3.5 Alerte et réparation | | |
| Règle 6.3.6 Sensibilisation des utilisateurs | | |
| Principe 6.4 Sauvegardes et journaux d’exploitation | « Maintenir un niveau de disponibilité et d’intégrité des systèmes d’information conforme aux exigences de sécurité » | Intendance |
| Règle 6.4.1 Politique de sauvegarde des informations | | |
| Règle 6.4.2 Protection et vérification des sauvegardes | | |
| Règle 6.4.3 Sécurité des sauvegardes de recours | | |
| Règle 6.4.4 Protection physique des sauvegardes | | |
| Règle 6.4.5 Archivage | | |
| Règle 6.4.6 Tenue de journaux d’exploitation | | |
| Règle 6.4.7 Consignation des anomalies | | |
| Règle 6.4.8 Audit des journaux d’exploitation et d’anomalies | | |
| Principe 6.5 Gestion des réseaux | « Assurer la protection de l’information dans les réseaux et la protection de l’infrastructure » | Gestion des réseaux |
| Règle 6.5.1 Mesures de sécurité des réseaux | | |
| Principe 6.6 Manipulation et sécurité des supports | « Prévenir les dommages causés au support de l’information et l’interruption de service » | Manipulation et sécurité des supports |
| Règle 6.6.1 Gestion des supports informatiques amovibles | | |
| Règle 6.6.2 Mise au rebut des supports informatiques contenant des informations sensibles | | |
| Règle 6.6.3 Transport et stockage des supports informatiques contenant des informations sensibles | | |
| Règle 6.6.4 Sécurité des documentations de systèmes X | | |
| Principe 6.7 Echanges d’informations et de logiciels | 1. « Empêcher toute perte, modification ou utilisation abusive des informations échangées entre des organisations de santé » 2. « Sécuriser les relations électroniques établissement – fournisseur (commerce électronique) » | Echanges d’informations et de logiciels |
| Règle 6.7.1 Rédaction, mise en œuvre et contrôle de la politique de sécurité pour l’accès au DIS, le stockage et l’échange d’informations au sein du DIS | | |
| Règle 6.7.2 Sécurité des supports pendant leur transport | | |
| Règle 6.7.3 Charte de sécurité pour l’utilisation de la messagerie électronique et d’Internet | | |
| Règle 6.7.4 Sécurité du commerce électronique | | |
| Règle 6.7.5 Sécurité des systèmes bureautiques | | |
| Règle 6.7.6 Sécurité des systèmes disponibles au public | | |
| Règle 6.7.7 Autres formes d’échange d’informations | | |

|  |  |  |
| --- | --- | --- |
| Chapitre 7 Contrôle d’accès logique | | |
| Principe 7.1 Expression des exigences de l’établissement en matière de contrôle d’accès  logique | « Contrôler l’accès aux informations » | Exigences de l’entreprise concernant le contrôle des accès |
| Règle 7.1.1 Politique d’autorisation | | |
| Règle 7.1.2 Contractualisation des exigences de contrôle d’accès logique | | |
| Règle 7.1.3 Règles de contrôle d’accès logique | | |
| Principe 7.2 Gestion des accès des utilisateurs | « Prévenir tout accès non autorisé aux systèmes d’information de l’établissement » | Gestion des accès utilisateurs |
| Règle 7.2.1 Registre des utilisateurs | | |
| Règle 7.2.2 Audit périodique du registre des utilisateurs | | |
| Règle 7.2.3 Formalisation des responsabilités en matière de contrôle d’accès logique | | |
| Règle 7.2.4 Gestion des autorisations d’accès aux fonctions privilégiées | | |
| Règle 7.2.5 Référentiel d’authentification des utilisateurs | | |
| Règle 7.2.6 Authentification des utilisateurs internes à l’établissement | | |
| Règle 7.2.7 Authentification des utilisateurs externes à l’établissement | | |
| Règle 7.2.8 Gestion des mots de passe des utilisateurs | | |
| Règle 7.2.9 Stockage des mots de passe | | |
| Règle 7.2.10 Revues des autorisations des utilisateurs | | |
| Principe 7.3 Responsabilités des utilisateurs | « Obtenir la coopération des utilisateurs pour maintenir l’efficacité du contrôle d’accès » | Responsabilités des utilisateurs |
| Règle 7.3.1 Utilisation des authentifiants | | |
| Règle 7.3.2 Protection de la confidentialité des mots de passe | | |
| Règle 7.3.3 Protection des équipements laissés sans surveillance | | |
| Principe 7.4 Contrôle d’accès logique au niveau des réseaux | « Protéger l’accès aux services fournis en réseau » | Contrôle de l’accès aux réseaux |
| Règle 7.4.1 Établissement de droits d’accès aux réseaux informatiques | | |
| Règle 7.4.2 Charte d’utilisation des réseaux | | |
| Règle 7.4.3 Chemin d’accès obligatoire et cloisonnement des réseaux | | |
| Règle 7.4.4 Authentification des utilisateurs lors des connexions distantes | | |
| Règle 7.4.5 Restriction d’accès aux ports utilisés pour la télémaintenance | | |
| Règle 7.4.6 Cloisonnement des réseaux et contrôle des flux | | |
| Règle 7.4.7 Translation d’adresses | | |
| Règle 7.4.8 Identification des caractéristiques de sécurité des services en réseau | | |
| Règle 7.4.9 Audit périodique des règles de contrôle d’accès aux réseaux | | |
| Principe 7.5 Contrôle d’accès logique au niveau des systèmes d’exploitation | « Prévenir les accès non autorisés aux ordinateurs (postes de travail, serveurs, éléments d’infrastructure…) » | Contrôle de l’accès aux systèmes d’exploitation |
| Règle 7.5.1 Procédure de connexion au poste de travail | | |
| Règle 7.5.2 Authentification du poste de travail | | |
| Règle 7.5.3 Gestion des mots de passe d’accès au système d’ exploitation | | |
| Règle 7.5.4 Restriction de l’accès aux utilitaires systèmes | | |
| Règle 7.5.5 Limitation de durée d’une session inactive | | |
| Règle 7.5.6 Limitation des horaires de connexion | | |
| Principe 7.6 Contrôle d’accès logique au niveau des applications | « Prévenir les accès non autorisés aux informations et aux fonctionnalités applicatives » | Contrôle de l’accès aux applications |
| Règle 7.6.1 Restriction d’accès aux informations | | |
| Règle 7.6.2 Isolation des systèmes de haute sensibilité | | |
| Principe 7.7 Supervision des accès et de l’utilisation des systèmes d’information | « Détecter des activités non autorisées » | Surveillance des accès aux systèmes et de leur utilisation |
| Règle 7.7.1 Journalisation des événements | | |
| Règle 7.7.2 Informations élémentaires pour le suivi des risques | | |
| Règle 7.7.3 Indicateurs de risque sur les systèmes et réseaux | | |
| Règle 7.7.4 Surveillance des outils de journalisation | | |
| Règle 7.7.5 Synchronisation des horloges | | |
| Principe 7.8 Cas particuliers des postes nomades et du travail à distance | « Assurer le maintien d’un niveau de sécurité adéquat dans les accès réalisés depuis des postes nomades et dans les accès distants » | Informatique mobile et télétravail |
| Règle 7.8.1 Postes nomades | | |
| Règle 7.8.2 Travail à distance | | |

|  |  |  |
| --- | --- | --- |
| Chapitre 8 Développement et maintenance des applications et systèmes | | |
| Principe 8.1 Intégration de la sécurité dans les développements | 1. « Intégrer la sécurité dans les systèmes d’information » 2. « Intégrer la prise en compte de la sécurité dans la conduite des projets (exigences et mesures de sécurité) » | Exigences de sécurité des systèmes |
| Règle 8.1.1 Organisation pour la prise en compte de la sécurité dans les projets de  développement et de maintenance | | |
| Règle 8.1.2 Définition des exigences de sécurité et choix des mesures de sécurité à  mettre en œuvre | | |
| Règle 8.1.3 Développement des fonctions/mécanismes de sécurité et recette sécurité de l’application | | |
| Principe 8.2 Cadre de mise en œuvre des mécanismes applicatifs et procéduraux de sécurité | « Donner un cadre à la mise en œuvre des mécanismes applicatifs et procéduraux dans le développement, l’utilisation et la maintenance des systèmes, sous la forme d’une norme interne à respecter pour tous les éléments du  système d’information » | Sécurité des systèmes d’applications |
| Règle 8.2.1 Définition du cadre de référence pour la mise en œuvre des mécanismes de  Sécurité | | |
| Règle 8.2.2 Contrôles de validité des données d’entrée des applications | | |
| Règle 8.2.3 Contrôles des traitements | | |
| Règle 8.2.4 Validité des messages | | |
| Règle 8.2.5 Validation des données de sortie | | |
| Principe 8.3 Cadre de mise en œuvre des mécanismes cryptographiques de sécurité | « Donner un cadre à la mise en œuvre des mécanismes cryptographiques dans le  développement, l’utilisation et la maintenance des systèmes, sous la forme d’une norme interne à respecter pour tous les éléments du système d’information » | Mesures cryptographiques |
| Règle 8.3.1 Cadre de référence pour l’utilisation de mécanismes de cryptographie | | |
| Principe 8.4 Sécurité des logiciels en exploitation | 1. « Sécuriser les fichiers, logiciels et progiciels utilisés dans le système d’information » 2. « Définir les rôles et responsabilités dans le maintien de l’intégrité des composants du système d’information » | Sécurité des fichiers |
| Règle 8.4.1 Contrôles des logiciels opérationnels | | |
| Règle 8.4.2 Protection des données d’essai des systèmes | | |
| Règle 8.4.3 Contrôle de l’accès aux codes sources des logiciels | | |
| Principe 8.5 Sécurité des environnements de développement et d’assistance | « Sécuriser les activités de support et de maintenance » | Sécurité des environnements de développement et de soutien |
| Règle 8.5.1 Procédures de contrôle des modifications | | |
| Règle 8.5.2 Restrictions sur les modifications apportées aux progiciels | | |
| Règle 8.5.3 Voies secrètes et Troyens | | |
| Règle 8.5.4 Sous-traitance du développement de logiciels | | |

|  |  |  |
| --- | --- | --- |
| Chapitre 9 Gestion de la continuité | | |
| Principe 9.1 Prise en compte des exigences de l’établissement concernant la disponibilité | « Pallier les interruptions d’activités de l’établissement et protéger ses processus cruciaux contre les effets de sinistre majeur qu’il soit informatique ou non » | Aspects de la gestion de la continuité des activités de l’entreprise |
| Règle 9.1.1 Organisation de la continuité de l’établissement | | |
| Règle 9.1.2 Analyse des besoins de continuité | | |
| Règle 9.1.3 Réponse aux besoins de continuité | | |
| Principe 9.2 Mise en œuvre d’un plan de continuité | « Elaborer un plan de continuité opérationnel. » | 1. Création et mise en œuvre des plans de continuité 2. Cadre de planification de la continuité des activités de l’entreprise |
| Règle 9.2.1 Organisation de crise | | |
| Règle 9.2.2 Mesures conservatoires | | |
| Règle 9.2.3 Elaboration d’un Plan de Secours Informatique (PSI) | | |
| Règle 9.2.4 Les sauvegarde de recours | | |
| Règle 9.2.5 Elaboration de Plan de Secours de Ressources non informatiques (PSR) | | |
| Règle 9.2.6 Elaboration d’un Plan de Reprise des Activités | | |
| Règle 9.2.7 Fonctionnement en mode « secours » | | |
| Règle 9.2.8 Plan de retour à la normale | | |
| Principe 9.3 Maintien en conditions opérationnelles du plan de continuité de l’établissement | « Disposer des plans de continuité opérationnels » | Essai, maintien et réévaluation des plans de  continuité des activités de l’entreprise |
| Règle 9.3.1 Préservation de l’homogénéité du Plan de Continuité | | |
| Règle 9.3.2 Maintien en condition opérationnelle | | |

|  |  |  |
| --- | --- | --- |
| Chapitre 10 Respect de la réglementation externe et interne | | |
| Principe 10.1 Respect de la réglementation externe | « Eviter les infractions à toute obligation d’ordre pénal et civil, légal, réglementaire ou contractuel, et à toute exigence interne de sécurité » | Conformité aux exigences légales |
| Règle 10.1.1 Identification de la législation applicable et rédaction des procédures | | |
| Règle 10.1.2 Respect de la législation sur le traitement des données personnelles et le  respect de la vie privée : déclarations à la CNIL | | |
| Règle 10.1.3 Respect de la législation sur le traitement des données personnelles et le  respect de la vie privée : le droit d’information, d’accès, de rectification et d’opposition | | |
| Règle 10.1.4 Respect de la réglementation relative à la garantie de la confidentialité des  données de santé à caractère personnel | | |
| Règle 10.1.5 Respect de la réglementation relative à l’accès aux informations personnelles  détenues par les professionnels et les établissements de santé (décret du 29 avril 2002) | | |
| Règle 10.1.6 Respect de la réglementation relative au traitement des données  personnelles de santé à des fins médico-économiques et épidémiologiques | | |
| Règle 10.1.7 Respect de la législation relative à l’informatique et des systèmes  d’information | | |
| Règle 10.1.8 Respect de la législation relative à l’utilisation des moyens cryptographiques  et de la signature électronique | | |
| Règle 10.1.9 Respect des conditions et des durées légales de conservation | | |
| Règle 10.1.10 Collecte, conservation, restitution des éléments de preuve | | |
| Principe 10.2 Respect de la réglementation interne | 1. « S’assurer que les procédures et les systèmes sont conformes à la politique de sécurité » 2. « S’assurer que les procédures de sécurité sont bien respectées au travers d’évaluations régulières » | Examen de la politique de sécurité et de la conformité technique |
| Règle 10.2.1 Conformité à la politique de sécurité | | |
| Règle 10.2.2 Contrôle de conformité technique | | |
| Principe 10.3 Considérations sur les audits des systèmes | 1. « Eviter toute perturbation causée ou subie par le processus d’audit » 2. « Eviter l’utilisation abusive des résultats de l’audit » | Considérations sur les audits des systèmes |
| Règle 10.3.1 Procédures d’encadrement des audits techniques | | |

Chapitre

Principe

Objectif

Correspondance avec la norme ISO 17799

Règle

* 1. Les rôles des PS :
     + 1. Médecin unité de soins :
  + Rôle

Il consulte des informations :

* les informations concernant le patient qu’il prend en charge, notamment les résultats d’examens qui proviennent des systèmes de gestion de laboratoire, les comptes rendus médicaux et médico -techniques qui sont tapés par les secrétaires ;
* son agenda (gestion des rendez-vous). Il saisit des informations concernant le patient qu’il prend en charge, notamment :
* Observations ;
* Demandes d’actes médico-techniques, de soins, prescription de médicaments ;
* Saisies des données pour le PMSI.

Il valide les comptes -rendus médicaux saisis par les secrétaires.

* + Données accédées :

Il a accès aux dossiers des patients actuellement pris en charge dans l’unité de soins à laquelle il est rattaché, mais aussi au dossier des patients qui ONT ETE pris en charge par l’unité de soins à laquelle il est rattaché.

Dans certains cas, les médecins des unités de soins ont accès à l’ensemble des dossiers des patients de l’établissement, que le patient soit présent ou pas. C’est le cas dans certains établissements de « spécialité » (CHS, CLCC).

* + Exceptions :

Pour des raisons de service, il peut être amené à accéder au dossier d’un patient qui n’est pas pris en charge dans son unité de soins. Généralement, le cas se produit lorsque le médecin est de garde et qu’il est sollicité par une autre unité de soin que celle à laquelle il est rattaché.

* + - 1. Brancardiers :

Si leur rôle logistique est essentiel et souvent mal compris (insuffisance d’effectifs), ils ont assez peu d’interactions avec le SI.

* Consultation de la liste de travail de brancardage (incluant transport des patients et des dossiers médicaux) et ou des modalités;
* Validation de l’exécution d’une course (début, fin –aller et retour du patient).
  + - 1. Pharmaciens :

Les coopérations entre acteurs relatives à la dispensation nominative de médicaments impliquent :

* Une prescription nominative d’administration de médicaments par le médecin demandeur (prescripteur) ;
* Une analyse pharmacologique de la prescription par le pharmacien (analyse des incompatibilités et des interactions médicamenteuses;
* Une délivrance nominative des médicaments;
* Une administration du médicament au patient (généralement réalisée par une infirmière);
* Un relevé d’administration (dans le cas de l’administration de stupéfiants).

Les pharmaciens sont chargés d’effectuer l’analyse pharmacologique des prescriptions nominatives des patients (rédigées par les médecins prescripteurs), au vu des éléments de dossiers nécessaires. En cas d’analyse positive, il demande au préparateur de satisfaire la demande de médicaments, sinon, il suggère une modification de la prescription au prescripteur. Il archive la prescription.

* + - 1. Aides-soignants et agents hospitaliers :

Leurs fonctions sont des fonctions d’assistance aux différentes catégories de personnel et dépendent pour beaucoup de spécificités d’organisations locales. Pour l’essentiel, on peut dire qu’ils interagissent avec le SI au niveau de :

* Création des identités (serveur d’identité)
* Délivrance des rendez-vous
* Accueil des patients (vérification du rendez-vous et notification de l’arrivée)
* Inscription
* Gestion des repas
* Récupération d’examens antérieurs
* Saisie des éléments de facturation des actes
* Distribution des résultats
  + - 1. Cadres médico-techniques de radiologie :

Nous incluons sous ce chapitre aussi bien les cadres supérieurs médico -techniques que les cadres médico -techniques. Leurs fonctions sont sensiblement les mêmes que leurs homologues infirmiers, du point de vue des charges administratives et de gestion (des ressources humaines et matérielles). Il faut y ajouter les fonctions propres aux techniciens en radiologie. Du point de vue de la programmation des rendez-vous, ce sont généralement les seuls habilités à fermer ou ouvrir une ressource ou à pratiquer une surréservation (surbooking).

* 1. Les scénarios de la gestion d’accès logique :
     1. Modification des rôles activés :

L'utilisateur a la possibilité d'activer/désactiver les rôles dont il a accès, pour cela, il faut qu'il fasse une demande de modification au niveau du système. Le système alors :

* Génère les traces de l'utilisateur (authentification, date rôles activés/désactivés..);
* Vérifie que les rôles demandés simultanément ne sont pas incompatibles;
* Indique à l’utilisateur la date, l’heure et les rôles activés lors de la dernière connexion réussie ;
* Calcule les droits d’accès de l’utilisateur.
  + 1. Clôture de session :

Lors d’une clôture de session, le système génère une trace de clôture (même informations que pour l’ouverture).

* + 1. Accès à une ressource par exception au contrôle d’accès :
* Lorsqu’un utilisateur se voit refuser un accès (opération refusée sur une ressource), le système vérifie si son rôle est autorisé à utiliser le mécanisme d’exception ;
* Si c’est le cas, le système lui propose les rôles qu’il peut demander à titre exceptionnel.
  1. Les scénarios d’administration des autorisations :
     1. Création du compte d’un utilisateur interne :

Lors de l’embauche d’un nouveau membre du personnel, un compte personnel et nominatif doit lui être créé sur le système d’information de l’établissement. Dans la mesure du possible, un identifiant unique pour l’ensemble des composants du SI sera attribué à cet utilisateur. Des authentifiants correspondant aux différents canaux d’accès qu’il est susceptible d’utiliser lui sont également attribués. Si un mot de passe est utilisé comme authentifiant, l’utilisateur devra le modifier à sa première ouverture de session.

A la fin de ce scénario, l’utilisateur ne dispose toujours d’aucune autorisation.

* + 1. Création du compte d’un intervenant externe :

Lorsqu’un intervenant externe (prestataire, patient, PS en réseau…) a un besoin légitime d’accéder aux systèmes d’information de l’établissement, un compte personnel et nominatif doit lui être créé. Préalablement à toute création de compte pour un intervenant externe, une convention ou un document à caractère contractuel doit être signé. Ce document doit définir les engagements réciproques de l’utilisateur externe et de l’établissement, et notamment quels seront les droits accordés à l’utilisateur externe.

Des authentifiants correspondant aux différents canaux d’accès que l’utilisateur externe est susceptible d’utiliser lui sont également attribués. Si un mot de passe est utilisé comme authentifiant, l’utilisateur devra le modifier à sa première ouverture de session.

A la fin de ce scénario, l’utilisateur ne dispose toujours d’aucune autorisation.

* + 1. Suppression d’un compte :

Lorsqu’un utilisateur n’a plus de motif légitime pour accéder au système d’information de l’établissement, son compte doit être invalidé (c’est à dire qu’il existe toujours, mais ne permet plus d’ouvrir de session).

Une fois que les opérations nécessaires à la sauvegarde, à l’archivage et au respect des obligations de traçabilité sont effectuées, le compte peut être détruit.

L’invalidation d’un compte peut aussi être utilisée à titre temporaire lors d’une absence de longue durée d’un utilisateur.

* + 1. Définition des rôles :

Les rôles sont définis de manière à refléter un métier, une fonction, une mission… Ils sont toujours définis indépendamment des utilisateurs.

* + 1. Affectation d’un utilisateur à un élément de structure avec un rôle :

L’attribution de droits à un utilisateur est réalisée en créant les affectations nécessaires [utilisateur, élément de structure, rôle].

L’utilisateur dispose alors de l’ensemble des autorisations attribuées à chacun de ses rôles.

1. Référence

[[1]:](#ISO11) ISO 7498-2, traduction AFNOR

[[2]:](#ISO22) ISO/IEC IS 2382-8 (1998), AFNOR

[[3]:](#Explic) Guide d’autoévaluation de la sécurité du système d’information : Outil d’autoévaluation

1. Webographie
   * <http://www.gmsih.fr/> (<http://www.anap.fr/>)