Groupement pour la Modernisation du Système d'Information Hospitalier

Aide à la détermination des services pour les établissements de santé

Version 1.0

GMSIH – 374, rue de Vaugirard – 75015 Paris. Tel : 01 48 56 72 73. Fax : 01 48 56 07 70

Auteurs du document :	Responsable Qualité
GMSIH	

Date	Version	Commentaires	Statut
10/02/2004	1.0	Publication	Validé

Sommaire

Références

Le GMSIH a produit les références suivantes relatives aux services de sécurité des Systèmes d'Information des établissements de santé :

[0] Synthèse de l'étude Services de sécurité

[1] Aide à la détermination des services de sécurité pour les établissements de santé In21LMTHv1

[2] Profil Fonctionnel de Sécurité : Domaine de sécurité- Coopération inter établissements In21PFSCIEv1

[3] Profil Fonctionnel de Sécurité : Domaine de sécurité- Portail Ville-hôpital In21PFSPVH1

[4] Profil Fonctionnel de Sécurité : Domaine de sécurité- SIH In21PFSSIHv1

[5] Profil Fonctionnel de Sécurité : Domaine de sécurité- Réseau de santé In21PFSRSv1

[6] Profil Fonctionnel de Sécurité : Domaine de sécurité- Centre 15 In21PFSCT15v1

[7] Profil Fonctionnel de Sécurité : Domaine de sécurité- SIH hébergé In21PFSHEBv1

[8] Visite guidée des documents sur les mécanismes de sécurité In21Visite guidéev1

[9] Classement des services de sécurité In21CLASSV1

[10] Mise en œuvre des mécanismes par PFS In21MEOv1

[11] Mécanismes d'authentification In21LT1v1

[12] Guide méthodologique. Elaboration d'un plan de secours In21LT2v1

[13] Mécanisme de chiffrement In21LT3v1.1

[14] Mécanisme de scellement et de signature In21LT4v1.1

[15] Mécanismes de traçabilité In21LT5v1.1

[16] Mécanismes de contrôle d'accès et de gestion des autorisations In21LT6v1.1

[17] Sécurisation des postes et terminaux mobiles In21LT7v1.1

[18] Aide à l'élaboration des tableaux de bord In21TAB1.1

[19] Guide méthodologique : Intégration de la sécurité dans la gestion de projet In21ISPv1

[20] Trajectoire de migration opérationnelle In21TMOv1

1. Objectif du document

1.1. Le contexte d'élaboration

L'évolution de l'offre de soins et de son organisation autour de la prise en charge coordonnée du patient oblige à prendre en compte de plus en plus la collaboration entre établissements de santé et leurs différents partenaires (médecins de ville, réseau de santé, association,…), ainsi que la communication des informations de santé du patient (application de la Loi du 4 mars 2002) : l'interopérabilité et l'ouverture deviennent des caractéristiques majeures des systèmes d'information.

Ce contexte présente des enjeux structurants du point de vue de la sécurité :

- Garantir la confidentialité des informations personnelles à caractère médical des patients ;
- Garantir le respect d'une politique de sécurité par les SIS et les SIH impliqués dans l'échange de ces informations. Cette dernière définit l'ensemble des principes de sécurité juridiques, humains, organisationnels et techniques qu'il convient d'appliquer pour ces échanges ;
- Faire prendre conscience aux établissements des impacts de l'intégration croissante de l'informatique dans leurs activités, en terme de continuité de service, y compris pour les situations d'urgence ;
- Faire prendre conscience aux établissements que tout nouveau projet d'informatisation et notamment dans la « production des soins », doit comporter un volet sur la sécurité des systèmes.

L'étude « Services de sécurité »

Les objectifs de l'étude « Services de sécurité » sont les suivants :

- Définir les services de sécurité nécessaires à la mise en œuvre de la politique de sécurité cadre publiée par le GMSIH[1] en tenant compte :
  - Pour les SIH :

    - de la politique d'autorisation (gestion des autorisations, gestion des délégations, prise en compte du contexte patient) ;

    - de la confidentialité des échanges de données médicales ;

    - du rôle du patient en tant qu'acteur ;

    - du rôle et responsabilité des tiers (autorités de certification, infomédiaires / hébergeurs de dossiers médicaux) ;

    - archivage...
  - des priorités liées à la sélection des services à prendre en compte dans cette étude :.

    - L'objectif de l'étude étant de produire rapidement, une fois le cadre général établi, des recommandations de solutions de sécurité, des

[1] «Politique de Sécurité Cadre des Systèmes d'Information (PSC-SI) » publiée par le GMSIH

priorités d'étude quant au choix des services de sécurité retenus sont définies

- Recommander des solutions de sécurité en tenant compte des spécificités des établissements de santé :
  - proposition de solutions abordables pour les établissements (par exemple, étude des logiciels libres) ;
  - trajectoire de migration réaliste au regard du niveau de sécurité actuel de l'établissement, de son architecture technique, de son budget ;
  - dialogue avec les fournisseurs de solutions et les éditeurs ;
- Prendre en compte l'offre du GIP-CPS, dispositif de référence dans le domaine de la santé, en intégrant les besoins propres à l'établissement de santé ;
- Accompagner les recommandations de solutions par des recommandations organisationnelles et des aides méthodologiques.

1.2. Objectif du document

Ce document d'aide à la détermination des services de sécurité pour les ES est destiné aux personnes chargées dans les établissements hospitaliers d'étudier les besoins de sécurité et/ou de trouver les dispositifs adaptés permettant d'y répondre :

- Les responsables de la sécurité des systèmes d'information (RSSI), lorsque la fonction a été créée dans l'établissement conformément aux recommandations de la Politique de Sécurité Cadre des Systèmes d'Information (PSC-SI) ;
- Le médecin responsable du Département de l'Informatique Médicale ;
- Le responsable Système d'Information et Organisation de l'établissement ;
- Et tout collaborateur de l'établissement chargé d'intégrer la sécurité dans son système d'information actuel ou à venir.

Il a pour objectif d'aider les établissements de santé, notamment lorsqu'ils lancent des projets d'envergure pour la modernisation de leur système d'information,

- à identifier des besoins de sécurité adaptés aux enjeux de l'établissement et aux objectifs fixés au système d'information,
- à définir les besoins de sécurité de manière cohérente (pour la disponibilité, l'intégrité, la confidentialité, la preuve et le contrôle des informations et des applications), en fonction de l'architecture existante ou en construction,
- à choisir les services de sécurité répondant aux besoins de sécurité.

L'application de la démarche décrite dans ce guide a été réalisée dans chaque Profil Fonctionnel de Sécurité : le lecteur peut s'y reporter pour mieux appréhender la démarche.

La démarche suppose d'inscrire son action dans le cadre fondateur que constitue la Politique de Sécurité Cadre (PSC-SI) publiée par le GMSIH : il est donc utile de prendre connaissance des chapitres et principes de la PSC-SI avant d'engager l'étude des besoins et des services de sécurité.

Enfin, il convient de souligner auprès des utilisateurs de ce document que les Profils Fonctionnels de Sécurité élaborés avec la démarche décrite ici contiennent des cas génériques d'activités et d'architecture : ils constituent donc un point de départ que les RSSI vont approfondir lorsqu'ils auront à analyser leur propre contexte (analyse des risques et choix des services à mettre en œuvre).

2. Introduction à la gestion des risques liés au système d'information

2.1. Information et système d'information dans un établissement de santé

Avant même d'introduire les notions et concepts de sécurité des systèmes d'information, il convient de rappeler quelques définitions :

Etablissement de santé

L'établissement de santé se définit selon les articles L. 6111-1 et L.6111-2 du Code de la Santé Publique. L'article L 6111-2 en particulier indique :

« Les établissements de santé, publics ou privés, ont pour objet de dispenser, avec ou sans hébergement :

- des soins de courte durée ou concernant des affections graves pendant leur période aiguë en médecine, chirurgie, obstétrique, odontologie ou psychiatrie ;
- des soins de suite ou de réadaptation dans le cadre d'un traitement ou d'une surveillance médicale à des malades requérant des soins continus ;
- des soins de longue durée, comportant un hébergement, à des personnes n'ayant pas leur autonomie de vie dont l'état nécessite une surveillance médicale constante et des traitements d'entretien. »

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.

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.

2.2. Sécurité de l'information

La Politique de Sécurité cadre définit la sécurité de l'information, et, par extension, la sécurité du système d'information automatisé, comme étant la préservation de :

- sa **confidentialité** : faire en sorte que l'information ne soit accessible qu'aux personnes autorisées à y accéder ;

- son **intégrité** : protéger l'exactitude et l'intégrité de l'information et des méthodes de traitement ;
- 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 ;
- et les moyens de **preuve et contrôle** nécessaires aux utilisateurs pour accorder leur confiance dans l'information fournie.

2.3. Risque et sécurité

La PSC demande (principe 1.2.2) que l'établissement procède régulièrement à une évaluation de ses risques.

Risque et sécurité sont des termes qui reviennent dans le langage courant, mais qui recouvrent des notions très variées liées au danger, à l'incertitude de l'avenir. Il peut donc être utile d'en rappeler la définition.

Risque

La notion de sécurité est intrinsèquement liée à celle de risque. Le dictionnaire définit le risque comme étant :

- la possibilité, la probabilité d'un fait, d'un événement considéré comme un mal ou un dommage (par exemple, « les risques de guerre augmentent ») ;
- un danger éventuel plus ou moins prévisible ;
- le fait de s'exposer à un danger (dans l'espoir d'obtenir un avantage) : *on n'a rien sans risque* ;
- en droit, l'éventualité d'un événement ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage.

Ces différentes définitions donnent chacune une des facettes du risque. Une bonne démarche de sécurité doit toutes les prendre en considération :

- un risque est lié à un dommage potentiel : sa réalisation doit avoir un **impact** ;
- il est plus ou moins prévisible : le risque est d'autant plus grand que sa réalisation est certaine ;
- on peut prendre sciemment des risques : le risque est quelque chose que l'on peut gérer, et pas uniquement subir ;
- le risque fait appel à un événement indépendant de notre volonté, on ne pourra pas complètement le maîtriser.

Sécurité

Le Dictionnaire Littré définit la sécurité comme étant la « tranquillité d'esprit dans une situation où il y aurait sujet de craindre ». Cette définition fait appel à trois éléments qui interagissent les uns avec les autres :

La tranquillité d'esprit : pour le Dictionnaire, la sécurité n'est pas un état physique, ne se mesure pas à l'aide d'un thermomètre ou d'un baromètre, mais correspond à un état psychologique. On se sent en sécurité, qu'on soit réellement ou pas exposé à des risques.

Situation où il y aurait sujet de craindre : pour le Dictionnaire, le fait de se sentir en sécurité est directement opposé au fait d'être exposé à un risque. Le fait de se sentir malgré tout en sécurité peut alors avoir deux raisons :

- je me sens en sécurité parce que **je ne connais pas les risques** auxquels je m'expose (c'est souvent le cas du baigneur l'été qui s'expose au soleil sans être conscient des risques pour sa peau) ;
- je me sens en sécurité parce que **je maîtrise mes risques** : je les ai identifié, évalués et j'ai pris des mesures pour m'en protéger (c'est le cas du baigneur qui utilise une bonne crème solaire, qui fait attention à sa durée d'exposition, surveille l'apparition de coups de soleil pour les soigner immédiatement…).

2.3.1. Quels sont les risques liés aux systèmes d'information ?

Les risques auxquels sont exposés les systèmes d'information peuvent avoir trois types de cause : les accidents, les erreurs et la volonté de nuire.

On regroupe généralement sous **l'origine accidentelle** :

- les accidents physiques (incendie, dégâts de eaux…) ;
- les catastrophes naturelles (tempêtes, tremblements de terre…) ;
- les pannes de matériel ;
- les pertes de servitudes essentielles (alimentation électrique, réseau télécom, climatisation…) ;
- etc.

Les incidents **liés à des erreurs** seront classés selon que l'erreur a eu lieu :

- lors de l'utilisation du système (erreur de saisie, erreur d'interprétation de données…) ;
- lors de sa conception (erreur de conception, de modélisation…) ;
- lors de sa construction (bugs de programmation, mauvais paramétrage…).

La typologie des incidents **d'origine malveillante** peut être basée sur les objectifs visés par l'agresseur :

- l'atteinte à la vie privée,
- le sabotage,
- la fraude…

Ces objectifs sont réalisés par des moyens, parmi lesquels : l'intrusion illégale sur un système, le piratage de logiciels ou de matériels, la divulgation d'informations, l'utilisation de codes illégaux et l'atteinte à l'intégrité des informations. Ces attaques touchent les services, les infrastructures et les données.

Une liste des scenarii de risques propres aux établissements de santé est jointe en annexe.

Ce sont par exemple, dans le cadre de l'admission des patients:

- Impossibilité de procéder à l'admission au niveau du service (indisponibilité de l'application de gestion du dossier médical, indisponibilité de l'application de production des soins),
- Erreur d'identification du patient lors de son admission,
- Rupture de la confidentialité de l'admission d'un VIP ou d'un membre du personnel,
- Absence de trace de l'admission générale du patient.

2.4. Stratégies de gestion du risque

La gestion du risque est un acte de management consistant à définir la conduite que l'on décide d'adopter face à un risque.

Afin de simplifier la prise de décision, on utilise des méthodes permettant de quantifier des niveaux de gravité du risque : on cherchera en priorité à réduire les risques caractérisés par un **impact insupportable**.

L'approche la plus simple est de distinguer les risques majeurs des risques courants. Les risques courants sont les risques qui peuvent être amortis sans trop de difficulté dans la gestion courante de l'établissement. Les risques majeurs sont alors ceux qui poseraient des difficultés sérieuses à l'établissement s'ils venaient à se réaliser (risques graves ou critiques), voire mettraient en danger la survie même de ses activités (risques stratégiques).

Le principe 1.2.2 de la Politique de Sécurité Cadre (règles concernant **l'évaluation périodique des risques** et le **choix des mesures**) donne les principes de maîtrise des risques. Ces principes visent à aider l'établissement à définir ses priorités de réduction des risques.

2.4.1. Combiner prévention et protection

Un risque a été défini comme étant le croisement d'un impact et d'une possibilité de réalisation. Afin de réduire le risque, il est donc possible d'agir sur ces deux axes :

- La **prévention** vise à diminuer les possibilités de survenance du risque. Elle comprendra toutes les mesures destinées à limiter l'exposition au risque, les mesures de dissuasion et les mesures de prévention immédiate.

  Par exemple, les campagnes d'information et les mesures d'hygiène diminuent l'exposition à certaines maladies, les radars dissuadent les automobilistes de faire des excès de vitesse, le gardiennage et les caméras de surveillances dissuadent le voleur de passer à l'acte,…

- La **protection** vise à diminuer l'impact du risque. Elle comprend les mesures de détection, de protection directe, les moyens palliatifs (c'est-à-dire permettant de poursuivre les activités malgré l'incident) et le transfert du risque vers un tiers (assurance, clauses contractuelles, recours juridiques…).

  Par exemple, les systèmes de détection d'incendie permettent d'agir au début du feu, les extincteurs permettent de l'éteindre, la voiture de remplacement fournie par le garage est une solution palliative en cas d'accident du véhicule et l'assurance limite le coût d'un dégât des eaux.

2.4.2. Suivi / Tableau de bord

Pour être efficace, la gestion des risques suppose le suivi d'une part de l'évolution des risques encourus, et, d'autre part, des mesures de sécurité mises en place. A cette fin, des tableaux de bord sont généralement établis.

2.5. Pourquoi évaluer ses risques ?

L'analyse des risques consiste à :

- Evaluer la gravité des risques encourus en fonction de leurs conséquences sur les activités de l'établissement, au cas où le scénario de risque se réaliserait,

Elle a pour but de :

- **Déterminer une réponse aux risques (dispositifs de sécurité) adaptée au niveau de gravité des risques encourus** : si la gravité est faible, la réponse pourra être un dispositif de sécurité simple, si la gravité est forte, le dispositif trouvé devra être d'un niveau élevé.

Elle va servir à établir le niveau de besoin qu'il faut couvrir, et par conséquent, le niveau des dispositifs de sécurité à mettre en œuvre (du plus faible au plus fort), et à justifier les budgets correspondants.

3. Détermination des services de sécurité à mettre en œuvre pour répondre aux risques

3.1. Application de la Politique de Sécurité : principes prioritaires et services de sécurité adaptés

La Politique de Sécurité des Systèmes d'Information des Etablissements de Santé (PSC-SI) contient des principes et des règles de mise en œuvre de la politique de sécurité, classés par chapitre (par exemple : Contrôle d'accès logique).

Le **Guide d'Auto-Evaluation (GAE)** permet à un établissement de mesurer son niveau de sécurité par rapport aux recommandations portées par la PSC-SI. Il en déduit des **principes et des règles de sécurité à mettre prioritairement en œuvre** dans son propre contexte.

Cependant, **plusieurs services de sécurité peuvent permettre d'appliquer les principes prioritaires** : l'**analyse des risques** permet de retenir le **service adapté au niveau de risque** encouru pour le système d'information considéré.

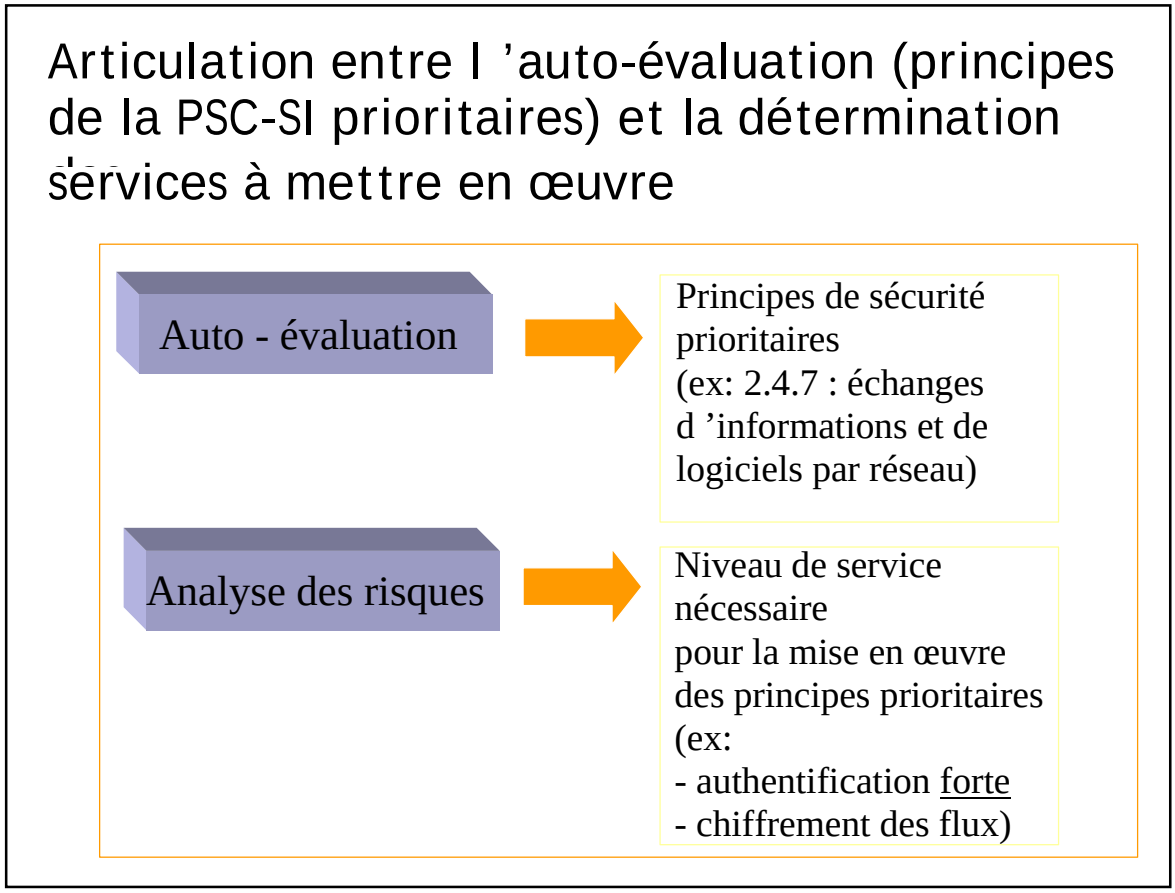


Schéma d'articulation entre les résultats de l'auto – évaluation et la détermination des services de sécurité à mettre en oeuvre

Alors que le Guide d'Auto-Evaluation (GAE) permet d'établir ses priorités dans la mise en œuvre de la politique de sécurité (par exemple mise en œuvre de la confidentialité des échanges), l'analyse des risques va permettre de déterminer le niveau des services de confidentialité mis en œuvre (par exemple, contrôle d'accès logique en interne, chiffrement lors des échanges via un réseau externe de données et de messages contenant des données médicales à caractère personnel).

3.2. Simplification de l'analyse des risques pour les établissements de santé

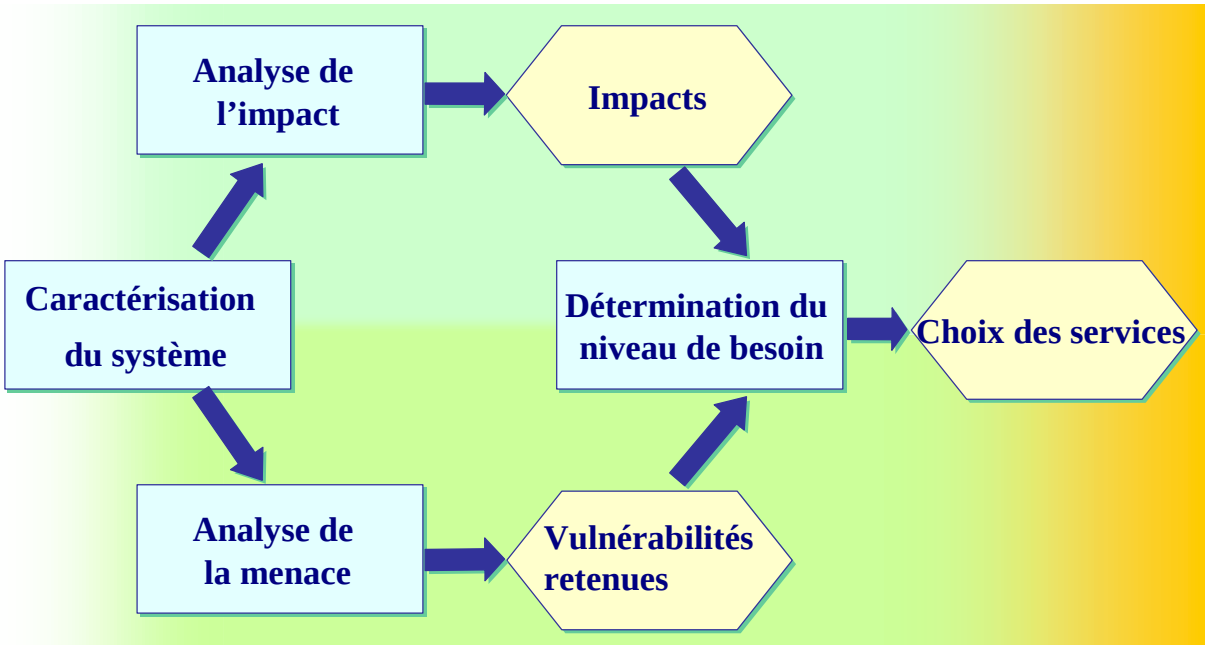
L'étude « Services de Sécurité » propose plusieurs aides à la réalisation d'une analyse des risques, en vue de simplifier la démarche pour les établissements :

- **Les profils fonctionnels de sécurité (PFS) des domaines de sécurité représentatifs** : un profil fonctionnel est l'« ensemble des besoins déterminés pour un domaine de sécurité et des services de sécurité répondant à ces besoins » , et les cas représentatifs retenus sont le SIH interne, le SIH avec un portail ville - hôpital, le SIH hébergé, le SIH en relation avec un réseau de santé, et la coopération entre établissements. Ils ont vocation à permettre au RSSI (Responsable de la Sécurité des Systèmes d'Information) et aux chefs de projet opérationnels de l'établissement de disposer d'analyses de risques ciblées déjà réalisées : si les activités et l'architecture correspondent à leur existant, les résultats des analyses de risques menées pour chaque PFS peuvent être réutilisés ;
- **Le présent document** comprenant
  - La présentation complète de la démarche utilisée pour élaborer les PFS,
  - **Deux aides pour l'application d'une démarche simplifiée :**
    - Une recommandation de démarche pour la détermination des besoins de sécurité liés à la mise en œuvre d'une nouvelle activité de l'établissement,
    - Une recommandation de démarche pour la détermination des besoins en cas de changement ou d'ajout de ressources techniques.

4. Présentation complète de la méthodologie utilisée pour déterminer les services de sécurité à mettre en oeuvre

La démarche générale de détermination des services de sécurité conduit à déterminer les services de sécurité répondant aux besoins de l'établissement.

Elle est représentée dans le schéma suivant :



La partie haute du schéma est centrée sur l'étude des *activités*[2] *et des métiers de l'établissement* : **l'analyse de l'impact** consiste à caractériser les enjeux sécurité liés à chacune des activités, en évaluant l'impact sur ces activités qu'auraient des sinistres potentiels du système d'information.

La partie basse du schéma est centrée sur l'étude des faiblesses du système d'information, et de la manière dont des **menaces** sont susceptibles de se concrétiser en exploitant des **vulnérabilités**.

La démarche est présentée ci-après de manière détaillée, étape par étape.

[2] Dans le cadre de ce guide, il s'agit des activités de soins et des activités de support qui leur sont liées, tels que le pilotage de l'établissement, les activités liées à la vigilance et à l'épidémiologie,….

4.1. Caractérisation du système

La première étape consiste à fixer le périmètre et les caractéristiques du système d'information du domaine de sécurité, afin d'identifier les activités et les ressources entrant dans le champ de l'analyse des risques.

4.1.1. Identification des activités entrant dans le domaine de sécurité

L'établissement recense les activités médicales, administratives, logistiques,…, entrant dans le domaine de sécurité : le recensement peut se faire sur la base d'une identification d'activités se rattachant à des grands processus métiers, ou sur la base de toute démarche qui lui est habituelle pour identifier ses principales activités (activités retracées dans la comptabilité analytique, par exemple). L'exercice peut être également mené pour les activités du réseau de santé, ou pour les activités faisant l'objet d'une coopération inter - établissements.

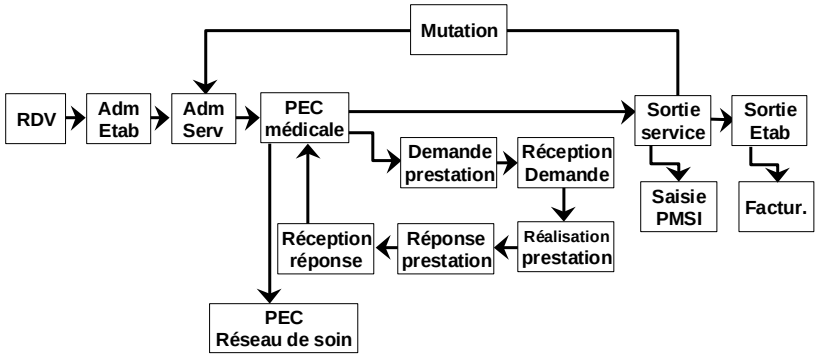
A titre d'exemple, est reproduit ci-dessous un extrait du Profil Fonctionnel de Sécurité (défini ci-après) du domaine de sécurité interne d'un établissement :

« Les activités de prise en charge du patient dans le cadre d'une hospitalisation sont centrées sur le fonctionnement d'une unité fonctionnelle, qui fait appel à des prestations complémentaires d'analyse (imagerie, laboratoire, exploration fonctionnelle…) ou de soins (kinésithérapie, soins infirmiers,…).

Un patient peut être hospitalisé :

- *suite à une prise de rendez-vous (par exemple fixée lors d'une consultation externe) ;*
- *suite à une admission décidée par le service d'urgences.*

Au jour fixé pour son hospitalisation, le patient est enregistré (dans la plupart des établissements) par le service d'admission générale, puis se rend dans le service qui le prend en charge.



La prise en charge médicale fait appel à un certain nombre de prestations complémentaires, qui permettent d'aider l' équipe médicale et soignante à établir le diagnostic et à soigner le patient.

La sortie de service peut être liée à deux motifs :

- la sortie définitive du patient de l'établissement ;

- le transfert dans un autre service (mutation).

Dans le cadre de la démarche utilisée, seule est réalisée l'identification des **activités sensibles**, c'est-à-dire des activités correspondant aux missions de l'établissement et/ou à ses obligations réglementaires, et à ses projets de développement stratégiques.

Prise de rendez-vous

Lors d'une prise de rendez-vous, la secrétaire du service concerné travaille essentiellement avec le serveur de rendez-vous de son service.

De plus en plus d'établissements ont mis en œuvre un serveur de rendez-vous central, qui permet de coordonner l'ensemble des agendas de l'établissement.

D'autre part, certains logiciels de gestion des rendez-vous sont directement connectés aux annuaires de ressources, structures et personnes, ainsi qu'au serveur d'identification des patients.

…»

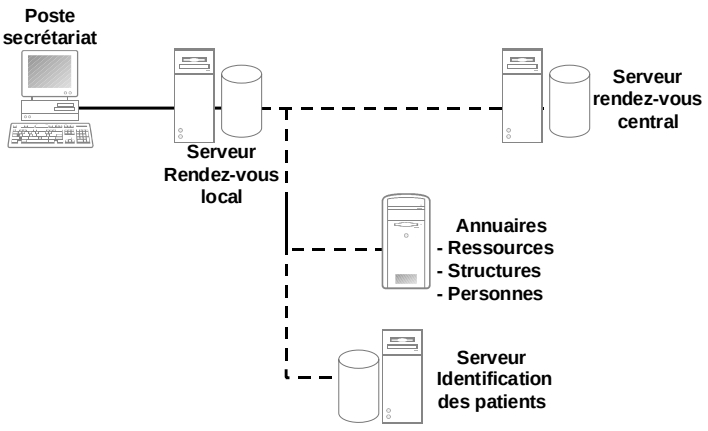
4.1.2. Identification des ressources du système d'information utilisées par l'activité

On entend par ressources l'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 la mettent en œuvre.

La caractérisation du système comprend une identification des ressources utilisées par l'activité, à un niveau de maille cohérent avec celui des activités.

L'extrait présenté ci-dessous indique le niveau de maille possible pour cette identification.

« Prise de rendez-vous



„

Dans ce schéma certains liens sont en pointillés, car représentant différentes options des systèmes d'information hospitaliers existants (par exemple, le serveur de rendez-vous local peut être relié ou non au serveur d'identification des patients et aux annuaires).

Dans le cas d'un établissement, le schéma représentera les ressources – machines, logicielles, réseau – existantes, ou prévues à court terme.

Une liste des ressources utilisées complète cette description :

Par exemple :

« Poste de travail (micro-ordinateur & tablette)

- *Console d'administration*
- *Poste agent*
- *Poste de maintenance*
- *Poste DIM*
- *Poste médecin*
- *Poste médecin vigilant*
- *Poste secrétariat*
- *Poste soignant*
- *Station graphique*

Réseau externe (WAN, Internet…)

- *Accès aux réseaux externes (Internet…)*

Réseau local (LAN)

- *Réseau local d'administration*
- *Réseau local de l'établissement »*

Il est à noter que les flux d'échanges d'information relatifs à une activité sont également recensés comme des ressources nécessaires au fonctionnement de l'activité. On regroupe tous les flux relatifs à une activité sous une même dénomination. Par exemple, les flux relatifs à l'admission du patient dans le service sont regroupés sous l'intitulé « flux Admission service ». Il convient de souligner que les flux d'échange recensés restent donc relativement génériques et ne sont pas du même niveau que ceux que l'on peut décrire dans la cartographie des processus et des flux menée par ailleurs par le GMSIH.

« Flux

- *Administration système*
- *Admission générale*
- *Admission service*
- *Admission urgences*
- *Demande de prestation*

- *PMSI*
- *Prise de rendez-vous*
- *Prise en charge médicale*
- *Réalisation de prestation*
- *Réception de demande de prestation*
- *Réponse suite à prestation*
- *Sortie de l'établissement*
- *Sortie du service*
- *Télémaintenance*
- *Vigilance (transmission des données) ».*

4.1.3. Architecture

La caractérisation comprend également une formalisation de l'architecture consistant en un schéma général de positionnement des ressources techniques systèmes et réseaux (voir paragraphe 3.4.1).

4.2. Analyse de l'impact

4.2.1. Analyse des enjeux de sécurité

L'analyse de l'impact consiste à caractériser les enjeux sécurité liés à chacune des activités, en évaluant l'impact sur ces activités qu'auraient des sinistres potentiels du système d'information.

Les sinistres potentiels correspondent à des atteintes à la disponibilité (D), à l'intégrité (I), à la confidentialité (C) et à la preuve et au contrôle (P) du système d'information.

Par exemple,

(les niveaux de classification sont présentés et explicités dans le commentaire de ce tableau)

Cas : Réseau de santé	***Processus : Inscription du patient***

Activités sensibles	***Nature du risque***	***Classification***			
		D	***I***	***C***	***P***
Sortie de prestation	*Impossibilité de communiquer les résultats de prestation aux membres du réseau concernés (indiquer le DMIA)*	***1***			
	Erreur dans la communication des résultats et la mise à jour du dossier (erreur d'identification du patient, erreur de résultat)		***3***		
	Non respect du secret médical			***3***	

Cas : Réseau de santé	***Processus : Inscription du patient***

Activités sensibles	***Nature du risque***	***Classification***			
		D	***I***	***C***	***P***
	Absence de traçabilité des prestations. Absence de preuve des prestations				***2***

Nature du risque

Les sinistres potentiels utilisés dans l'étude « Services de Sécurité » font l'objet d'un catalogue inséré en annexe du présent document : ils peuvent servir de base aux établissements pour la conduite de leur propre analyse des impacts.

Classification

Une **échelle d'évaluation des impacts** permettant d'évaluer le niveau d'impact :

Axes d'impact	Seuils d'impact			
	1 **limité**	2 **important**	3 **grave**	4 **critique**
Atteinte à la qualité des soins	Perturbation momentanée et limitée de l'organisation des soins	Perturbations limitées dans la délivrance des soins	Désorganisation des soins, ou atteinte limitée à l'état de santé d'un patient	Atteinte grave à l'état de santé d'un patient
Pertes financières	Pertes non significatives sur le plan financier	Pertes < 0,5% du budget global ou du chiffre d'affaires	Pertes de l'ordre de 0,5% du budget global ou du chiffre d'affaires	Pertes > 0,5 %du budget global ou du chiffre d'affaires
Engagement de la responsabilité	Plainte(s) de patient(s) signalant un dysfonctionnement	Plainte(s) de patient(s) signalant un dysfonctionnement grave, ou débouchant sur un recours	Plainte de patients débouchant sur une sanction disciplinaire à l'encontre d'un responsable à l'encontre d'un responsable	Plainte de patients débouchant sur la condamnation civile ou pénale d'un responsable d'établissement
Atteinte à l'image de l'établissement (auprès des patients, partenaires, tutelles, médecins de ville,…)	Divulgation limitée d'incidents	Altération significative de l'image de l'établissement	Altération très importante de l'image de l'établissement	Altération définitive de l'image de l'établissement

Exemple

- **Indisponibilité de la prise de rendez-vous pendant une demi-journée (nature de risque : Disponibilité)** :
  - Si le serveur de rendez-vous est centralisé, l'impact est **3** pour l'axe d'impact « atteinte à la qualité des soins » et l'axe «atteinte à l'image de marque de l'établissement vis-à-vis des patients » : la classification est D3 (à cette occasion on définit le délai maximum d'interruption admissible –DMIA- qui est de 1 heure),
  - Si le serveur de rendez-vous est propre à l'unité de soins (serveur décentralisé), l'impact est de **2** sur les mêmes axes d'impact : la classification est D2 (à cette occasion on recueille le DMIA qui est de 4 heures).

4.2.2. Classification des ressources

La caractérisation du système a conduit à déterminer les ressources du système d'information permettant la réalisation des activités.

Une ressource du système d'information peut être utilisée par plusieurs activités : la sensibilité de la ressource est celle de l'activité la plus sensible.

Exemple du serveur de rendez-vous central de l'établissement

- dans le cadre du domaine de sécurité du SIH interne :

Ressource	D	I	C	P
Serveur de rendez-vous central	**3**	1	3	1

- Dans le domaine de sécurité du SIH avec un portail ville-hôpital :

Ressource	D	I	C	P
Serveur de rendez-vous central	3	2	3	2

Le serveur de rendez-vous central a une classification I2 et P2, lorsqu'il met des données à la disposition des applications du portail Ville - Hôpital.

Exemple du réseau local interne à l'établissement :

Ressource	D	I	C	P
Réseau local d'administration	3	4	3	2
Réseau local de l'établissement	4	4	3	2

Le réseau local a la classification pour chaque critère (D,I,C,P) de l'activité (ou des activités) ayant la plus forte classification :

- D3 : demande, réponse ,… de prestation
- I4 : admission service, prise en charge médicale ,…
- C3 : (niveau général)
- P2 : prise en charge médicale, demande de prestation,…

4.3. Analyse de la menace

L'analyse de la menace a été réalisée dans le cadre de l'étude PSC-SI : les menaces génériques retenues pour réaliser le Guide d'Auto-Evaluation sont :

- Accident physique
- Perte de servitudes essentielles
- Perte de données

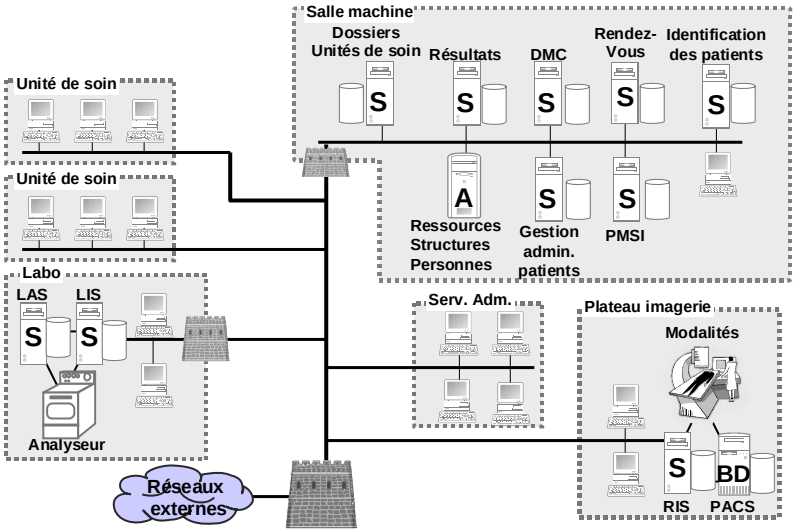
- Indisponibilité d'origine logique
- Divulgation d'informations en interne
- Divulgation d'informations en externe
- Abus ou usurpation de droits
- Fraude
- Reniement d'actions
- Non-conformité à la législation
- Erreurs de saisie ou d'utilisation
- Perturbation sociale

Les menaces ont été choisies en fonction de leur pertinence pour les systèmes d'information des établissements de santé: par exemple, on craint plus dans les systèmes d'information hospitaliers le détournement d'informations médicales à caractère personnel (« divulgation externe) ou le vol de matériels « attractifs » (micro-ordinateurs,…) que l'espionnage à distance (secteurs militaire, recherche et développement, et commercial fortement concurrentiel).

4.4. Vulnérabilités retenues

4.4.1. Architecture

La caractérisation du système conduit également à décrire l'architecture générale du système d'information : par exemple, l'architecture centralisée informatique d'un établissement.



L'architecture et les composants du système informatique comportent un certain nombre de vulnérabilités, c'est-à-dire de faiblesses qui représentent autant d'opportunité pour que le sinistre se réalise. Le fait, par exemple, d'utiliser Internet pour communiquer est un facteur de vulnérabilité du point de vue de la confidentialité des informations transportées.

4.4.2. Vulnérabilités retenues

Les vulnérabilités sont déterminées par un audit de la sécurité du système d'information.

En l'absence d'audit, par exemple dans le cadre d'un nouveau projet pour lequel l'architecture est en cours d'élaboration, il est conseillé de s'appuyer sur la liste des vulnérabilités retenues dans l'étude « Services de sécurité », qui est jointe en annexe.

4.5. Détermination des besoins de sécurité

Le besoin de sécurité d'une ressource est fonction du niveau d'impact de l'activité la plus sensible, éventuellement modifié par la prise en compte des vulnérabilités, comme le montre l'extrait suivant :

Ressource	Impact				Vulnérabilités	Axe DICP	Besoin retenu			
	D	I	C	P			D	I	C	P
Messagerie du réseau	1	2	3	1	Possibilité d'attaque par déni de service	D	1	2	4	2
					Possibilité d'attaque par introduction de logiciels malveillants (Troie, Ver,…)	DICP				
					Possibilité d'écoute passive	C				
					Possibilité d'infection virale	I				
					Possibilité pour des personnes non habilitées de tenter de bénéficier de droits qu'ils n'ont pas	ICP				
					Règles de sécurité logique non respectées sur les équipements réseau (routeurs,…)	ICP				

Dans ce cas, la messagerie du réseau passe par Internet : les possibilités d'attaque par introduction de logiciels malveillants, d'écoute passive, de tentative illicite de prise de connaissance du contenu, augmente le besoin de protection en confidentialité et en auditabilité du système (niveau 4).

Pour déterminer le niveau de besoin, une définition des niveaux de service a été réalisée (« grille de niveau de service », jointe en annexe).

La synthèse des besoins de sécurité par ressource est présentée dans l'étude « Services de sécurité » sous forme d'un tableau :

Flux

Ressource	D	I	C	P
Convocation à un rendez-vous	1	2	4	2
Demande d'inscription	1	2	4	1
Evaluation	1	2	2	1
Inscription du patient	2	3	4	2
Sortie	1	3	4	2
Sortie de prestation	1	3	4	2
Téléchargement du dossier	2	3	4	2

4.6. Choix des services de sécurité

Un service de sécurité se définit comme une « réponse possible à un besoin spécifique de sécurité. Il peut être assuré par un ou un ensemble de mécanismes de sécurité. »(source : méthode MEHARI – Clusif)

Pour les besoins de l'étude, une grille des services de sécurité a été réalisée : elle comporte deux parties jointes en annexe à ce document, en annexe 8.5. (définition des niveaux de sécurité) et 8.6 (liste des services classée par niveau).

Les services de sécurité retenus sont de trois types :

- Les services de sécurité mis en œuvre par des procédures ;
- Les services de sécurité mis en œuvre par des mécanismes techniques ;
- Les services de sécurité mis en œuvre par un ensemble de procédures et de mécanismes techniques ordonnés au sein d'un plan.

Il est important de souligner que les services de sécurité présentés dans les Profils Fonctionnels de Sécurité sont le résultat d'une application de cette grille : à un niveau de besoin de sécurité correspond un ou plusieurs services de sécurité prédéfinis.

L'étude des solutions réalisée dans le cadre de la présente étude permettra de proposer des solutions adaptées aux contraintes techniques, budgétaires et organisationnelles des établissements.

De plus, chaque établissement déterminera, après l'utilisation du guide d'autoévaluation, ses propres priorités de mise en œuvre des principes de sécurité de la politique de sécurité, et, par voie de conséquence, il retiendra en premier lieu les services de sécurité correspondants.[3]

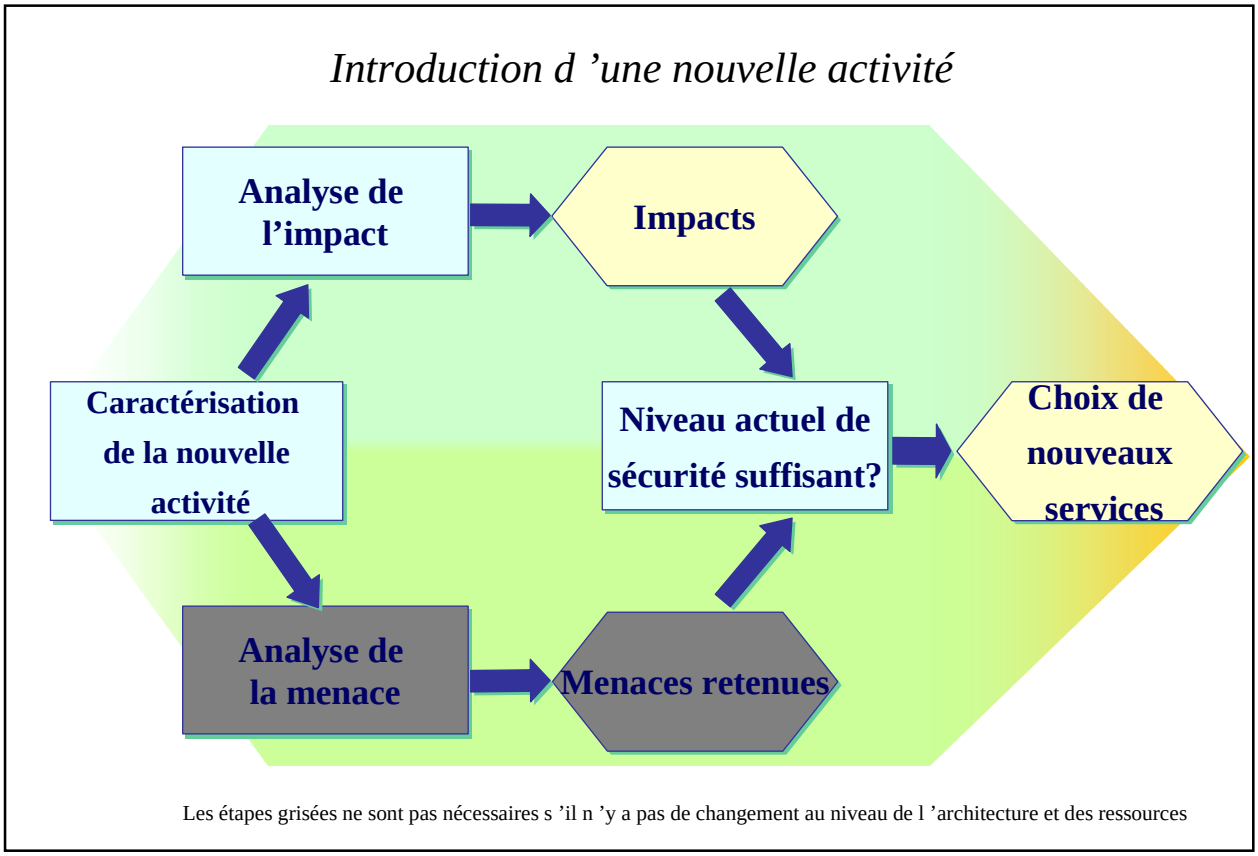
[3] Afin de faciliter la tâche des établissements une table des services comprenant la référence aux principes de la Politique de Sécurité Cadre a été établie (voir en annexe).

5. Détermination des besoins de sécurité liés à la mise en œuvre d'une nouvelle activité de l'établissement

5.1. Hypothèse de travail

Dans cette partie, on prend l'hypothèse que la nouvelle activité utilise les ressources actuelles du système d'information : au cas où le système d'information évoluerait pour prendre en compte cette nouvelle activité, il est conseillé de réaliser également la démarche décrite dans la partie 6 pour l'analyse des risques liés au changement ou à l'ajout de ressources techniques.

5.2. Démarche recommandée



En cas de création d'une nouvelle activité, il est conseillé aux établissements d'effectuer les tâches suivantes :

- Caractériser l'activité du point de vue fonctionnel, en suivant la démarche décrite au paragraphe 4.1.1 du guide,
- Réaliser l'analyse des impacts, en suivant la démarche décrite dans les paragraphes 4.2.1 et 4.2.2 du guide,

- Vérifier que les ressources du système d'information supportant cette nouvelle activité possèdent un niveau de sécurité suffisant pour répondre aux risques, en utilisant la démarche décrite au paragraphe 4.5.
- Au cas où le niveau actuel de sécurité ne conviendrait pas aux exigences déterminées lors de l'analyse d'impact, choix de nouveaux services répondant au besoin, en utilisant la démarche décrite au paragraphe 4.6.

Si la nouvelle activité est déjà décrite et évaluée dans l'un des Profils fonctionnels de sécurité, il est possible également de s'appuyer sur ce travail déjà réalisé, à condition qu'il corresponde au contexte de l'établissement.

Par exemple, la mise en place d'une coopération inter - établissements entraîne de nouvelles activités, dont voici l'évaluation pour l'une d'entre elles :

Fiche d'identification des activités sensibles

Cas : Coopération entre deux établissements	**Prestation réalisée par l'établissement B pour un patient pris en charge par l'établissement A**

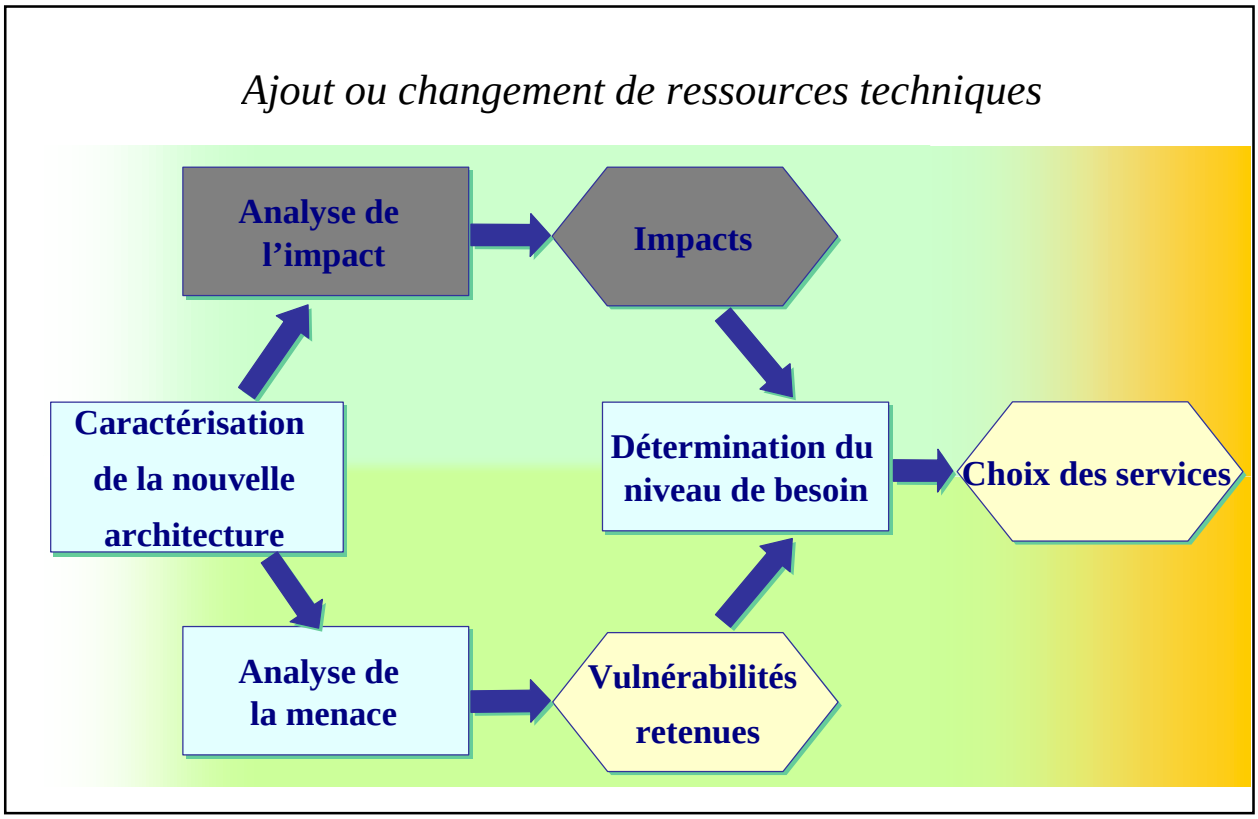
Activités sensibles	**Nature du risque**	**Classification**			
		D	**I**	**C**	**P**
Retour du patient à l'établissement A	• Impossibilité de rapatrier les informations concernant le patient	**2**			
	• Erreur dans les informations rapatriées (erreur d'identification du patient, informations incomplètes…)		**4**		
	• Non respect du secret médical			**3**	
	• Absence de traçabilité des tâches automatisées • Absence de signalement du téléchargement à l'émetteur • Absence de preuve de l'origine et de la validité des informations restituées par un professionnel de l'établissement				**3**

6. Démarche à appliquer pour la détermination des besoins en cas d'ajout ou de changement de ressources techniques

6.1. Hypothèses de travail

Dans cette partie, on prend l'hypothèse qu'à activités identiques, les ressources du système d'information évoluent (sauf les logiciels, qui restent à fonctionnalités égales). Au cas où les fonctionnalités des logiciels évolueraient, il convient de s'interroger sur la nécessité de réaliser également les activités prévues dans la partie 5 du présent document.

6.2. Démarche recommandée



Les étapes en grisé ne sont pas nécessaires en cas de changement de l 'architecture et des ressources

Dans le cas de changement ou d'évolution de ressources techniques (infrastructure systèmes, postes de travail, télécom,…), il est recommandé aux établissements de réaliser les activités suivantes :

- Caractérisation des nouvelles configurations supportant les activités, et de la nouvelle architecture, selon la démarche présentée en paragraphe 4.1.3 du guide,

- Revue des menaces à retenir (les menaces génériques restant cohérentes avec le système d'information cible), selon la démarche présentée en paragraphe 4.4.2 du guide ;
- Adaptation éventuelle du niveau de besoin en fonction des nouvelles vulnérabilités, selon la démarche présentée au paragraphe 4.5.44 du guide ;
- Choix des services, selon la démarche présentée en paragraphe 4.6 de la démarche.

Par exemple, l'ajout d'une configuration pour ouvrir l'accès aux réseaux publics de l'établissement A :

Ressource	Impact				Vulnérabilités	Axe DICP	Besoin retenu			
	D	I	C	P			D	I	C	P
Accès réseaux publics de A	3	4	3	3	Possibilité d'attaque par déni de service	D	3	4	4	2
					Possibilité d'attaque par introduction de logiciels malveillants (Troie, Ver,…)	DICP				
					Possibilité d'écoute passive	C				
					Possibilité d'infection virale	I				
					Possibilité de défaillance grave	D				
					Possibilité de destruction	D				
					Possibilité de répudiation des échanges	P				
					Possibilité pour des personnes non habilitées de tenter de bénéficier de droits qu'ils n'ont pas	ICP				

7. Bibliographie

[1] GMSIH. *Politique de sécurité cadre (version 1.0).* 2003.

[2] GMSIH. *Politique d'autorisation (version 1.0).* 2003.

[3] GMSIH. *Guide d'autoévaluation de la sécurité des systèmes d'information (version 1.0).* 2003.

[4] *MEHARI*, Clusif, 2000.

[5] GMSIH : *Les annuaires (version 1.0).2003*

8. ANNEXES

8.1. Echelle d'évaluation des impacts

La mesure du risque reposant sur l'évaluation des impacts de sinistres potentiels sur les missions de l'établissement, le GMSIH a construit une échelle d'évaluation dans le but d'aider les responsables des établissements à procéder à cette évaluation.

Cette échelle établit une classification des impacts de sinistres informatiques que les établissements pourraient être amenés à connaître, en distinguant :

- les risques dont l'impact est « acceptable » (seuils d'impact 1 et 2) ;
- les risques dont l'impact est « inacceptable » (seuils d'impact 3 et 4).

Axes d'impact	Seuils d'impact			
	1 **limité**	2 **important**	3 **grave**	4 **critique**
Atteinte à la qualité des soins	Perturbation momentanée et limitée de l'organisation des soins	Perturbations limitées dans la délivrance des soins	Désorganisation des soins, ou atteinte limitée à l'état de santé d'un patient	Atteinte grave à l'état de santé d'un patient
Pertes financières	Pertes non significatives sur le plan financier	Pertes < 0,5% du budget global ou du chiffre d'affaires	Pertes de l'ordre de 0,5% du budget global ou du chiffre d'affaires	Pertes > 0,5 %du budget global ou du chiffre d'affaires
Engagement de la responsabilité	Plainte(s) de patient(s) signalant un dysfonctionnement	Plainte(s) de patient(s) signalant un dysfonctionnement grave, ou débouchant sur un recours	Plainte de patients débouchant sur une sanction disciplinaire à l'encontre d'un responsable	Plainte de patients débouchant sur la condamnation civile ou pénale d'un responsable ou de l'établissement
Atteinte à l'image de l'établissement (auprès des patients, partenaires, tutelles, médecins de ville,…)	Divulgation limitée d'incidents	Altération significative de l'image de l'établissement	Altération très importante de l'image de l'établissement	Altération définitive de l'image de l'établissement

- les axes d'impact sont communs à la plupart des établissements de santé, publics et privés,
- les seuils d'impact – du niveau 1 « limité » au niveau 4 « critique » - font l'objet d'une définition : ils ne sont volontairement pas illustrés par des exemples d'impact, de manière à ne pas influencer l'évaluation de l'impact d'un sinistre potentiel pouvant se produire sur nombre d'activités de nature

totalement différente. De plus, le caractère relatif d'un niveau par rapport à un autre va permettre au responsable de l'activité de « relativiser » l'impact du sinistre par rapport à la bonne marche de l'ensemble de l'établissement.

8.2. Liste des vulnérabilités retenues pour l'étude « Services de sécurité »

Serveurs & services	Vulnérabilités retenues
Serveurs (matériel et système)	Manque de fiabilité des ressources
	Défaut de maintenance
	Possibilité de mal configurer, installer ou modifier les ressources
	Obsolescence des matériels
	Possibilité d'incompatibilité entre différentes ressources
	Ressources mal dimensionnées
	Maintenabilité des matériels/logiciels spécifiques
	Matériels obsolètes ou à configurations non évolutives
	Système permettant, par nature, d'accéder au données
	Système connecté à des réseaux externes
	Utilisation du matériel à un autre usage que celui prévu
	Possibilité de créer ou de modifier des commandes systèmes
	Possibilité d'implanter des programmes pirates
	Non respect de la sécurité logique (accès aux fonctions système)
Services applicatifs (logiciel)	Mauvaise conception, mauvaise installation des logiciels
	Mauvaise gestion des versions et configurations logicielles
	Possibilité d'utiliser une faille (porte dérobée) dans un programme
	Modules applicatifs ayant des droits excessifs sur les données
	Possibilité de modifier ou de changer les applicatifs
	Possibilité d'effacer ou de modifier les programmes
	Possibilité d'infection virale
	Possibilité d'existence de fonctions cachées
Messagerie, accès Internet	Systèmes favorisant une diffusion facile de l'information
	Système par nature accessible et utilisable par tous
	Système favorisant l'introduction de contenus illicites et de programmes malveillants
	Possibilité d'utilisation illégale d'Internet (condamnation pénale,…)

Postes, équipements mobiles	Vulnérabilités retenues
Micro-ordinateurs et tablettes	Possibilité que les systèmes fonctionnent avec des logiciels copiés illicitement ou contrefaits
	Système permettant de stocker un grand nombre d'informations sensibles dans un contenant réduit
	Possibilité de copier facilement des logiciels ou progiciels
	Logiciels attractifs « grand public »
	Possibilité d'infection virale
	Matériels attractifs (valeur marchande, technologique, stratégique)
	Système permettant un échange facile de l'information
PDA	Système permettant de stocker un grand nombre d'informations sensibles dans un contenant réduit
	Matériels attractifs (valeur marchande, technologique, stratégique)
	Possibilité d'infection virale
	Possibilité de perdre facilement des données (mécanisme de « reset », panne de piles)
	Possibilité de contournement des mécanismes de sécurité (mots de passe…)
	Possibilité de d'intercepter les informations transportées (liaisons radios, infrarouge)
Réseau interne	**Vulnérabilités retenues**
Réseau LAN	Possibilité de mal configurer, installer ou modifier les ressources
	Règles de sécurité logique non respectées sur les équipements réseau (routeurs,…)
	Sous-dimensionnement du réseau local
	Défaut de protection physique des installations entraînant destruction (armoires de câblage…)
	Possibilité de pose de dispositifs de communication non contrôlés
	Possibilité d'agir sur les données transmises par l'intermédiaire du media de communication
	Connexion du réseau interne au réseau externe
Réseau sans fil	Facilité pour un tiers de capter les informations transportées
	(+ voir ci-dessus)
Réseau externe (Internet)	**Vulnérabilités retenues**
	Possibilité de défaillance grave
	Possibilité de destruction

	Possibilité d'écoute passive
	Possibilité d'attaque par déni de service
	Possibilité d'attaque par introduction de logiciels malveillants (Troie, Ver,…)
	Possibilité d'attaque anti-virale
	Possibilité de répudiation des échanges
	Possibilité pour des personnes non habilitées de tenter de bénéficier de droits qu'ils n'ont pas

8.3. Table de correspondance entre les services de sécurité et les principes de la Politique de Sécurité PSC-SI

Note :

Les tables de correspondance seront complétées après validation des PFS.

8.3.1. Services permettant d'assurer la disponibilité

SERVICES DE SECURITE (disponibilité)	**REFERENCE PRINCIPE PSC**
Contrat de maintenance	2.3.2 2.6.1 2.6.2 2.6.4
Contrat de service (interne, externe) – fourniture de configurations de remplacement	1.2.4 (règle 6)
Détection d'intrusion	2.5.4 2.5.7
Contrôle de contenu	2.5.4
Disques à tolérance de pannes	2.4
Protection antivirale	2.4.3
Enregistrement haute sécurité, mirroring	2.4
Haute disponibilité (équilibrage de charges, doublement des configurations)	2.4
Filtrage des flux	2.4.5 ? 2.5.4
Maintenance sécuritaire (patchs)	2.4.1
Procédures de reprise sur incidents	2.7.2
Reprise automatisée sur incidents	2.7.2
Plan de sauvegarde (de production, de secours)	2.4.4
Plan de secours informatique et réseaux	2.7.2
Plan de gestion des incidents	2.2.3 2.4.4
Plan de communication de crise	2.7
Gestion de la documentation	2.4.1
Gestion automatisée de la documentation	2.4.1
Supervision des réseaux (procédures manuelles)	2.4.5
Supervision des réseaux (alertes automatisées)	2.4.5
Supervision des réseaux avec corrélation d'événements (détection, intrusion, filtrage)	2.5.4
Automatisation de l'exploitation	2.4.1

SERVICES DE SECURITE (disponibilité)	REFERENCE PRINCIPE PSC
Gestion de configuration	2.4.1
Contrôle d'accès physique	2.3.1 2.3.2 2.3.3
Procédure d'habilitation du personnel technique	2.2.1 2.2.2
Sécurité physique des équipements (réseaux, serveurs,..)	2.3.2

8.3.2. Services de protection de l'intégrité des données

SERVICES DE SECURITE (intégrité)	REFERENCE PRINCIPE PSC
Accusé réception	2.6.2
Authentification des personnes	2.5.2 2.5.4
Authentification des services	2.5.2
Authentification forte des personnes	2.5.1 2.5.2 2.5.8
Authentification forte des services	2.5.2
Chiffrement des échanges	2.4.7
Confidentialité des données (chiffrement, anonymat)	2.6.3
Contrôle de contenu	2.5.4
Contrôle d'accès logique (mise en œuvre du modèle de la PA)	2.5.4 2.5.5 2.5.6
Contrôle d'intégrité logique du réseau	2.5.4
Gestion des profils	2.5.2
Gestion des autorisations	2.5.2
Contrôle d'accès logique aux fonctions d'administration	2.5.5
Protection contre le rejeu et contre les doubles traitements des flux	2.6.2
Protection contre les modifications impropres ou illicites de configuration	2.6.4 2.6.5
Gestion de configuration	2.4.1 2.4.2
Gestion automatisée de la conformité de la configuration	2.6.4
Protection anti-virale	2.4.3
Plan de gestion des incidents (détection, traitement, investigation)	2.2.3 2.4.4

SERVICES DE SECURITE (intégrité)	**REFERENCE PRINCIPE PSC**
Scellement (données sensibles, flux)	2.1.2 2.4.7 2.6.2 2.6.3
Signature électronique	2.1.2 2.4.7 2.6.2 2.6.3
Sensibilisation des utilisateurs	1.2.3
Activation de la procédure automatisée de roll-back pour la base de données	2.6.2
Journalisation des saisies	2.5.7 2.6.1
Maintenance sécuritaire (patchs)	2.4.1
Contrôle conformité configuration	2.6.4
Plan de sauvegarde	2.4.4 2.7.2
Reprise automatisée sur incident	2.7.2
Filtrage des flux	2.5.4
Détection d'intrusion	2.5.4 2.5.7
Contrôle d'intégrité physique du câblage	2.3.2
Supervision des réseaux (alertes automatisées)	2.4.5 2.5.7
Supervision des réseaux avec corrélation d'événements (détection, intrusion, filtrage)	2.5.4
Procédure d'habilitation du personnel technique	2.2.1 2.2.2

8.3.3. Services de protection de la confidentialité

SERVICES DE SECURITE (confidentialité)	**REFERENCE PRINCIPE PSC**
CONFIDENTIALITE	
Identification de l'origine du flux	2.4.5 2.6.2
Authentification des personnes	2.5.2 2.5.4 2.5.5 2.5.6
Authentification des services	2.5.2
Authentification forte des personnes	2.5.1 2.5.2 2.5.4 2.5.5 2.5.6
Authentification forte des services	
Authentification mutuelle de l'émetteur et du destinataire du flux	2.6.2
Contrôle d'accès logique (mise en place de la Politique d'Autorisation de la PSC)	2.5.6
Charte	1.3.3 2.8.2
Chiffrement des échanges	2.4.7
Confidentialité des données (chiffrement, anonymat)	2.6.3
Contrôle de contenu	2.5.4
Gestion des profils	2.5.2
Gestion des autorisations	2.5.2
Habilitation des sous-traitants	1.2.4
Contrôle d'accès logique aux fonctions d'administration	2.5.2 2.5.4 2.5.5
Sensibilisation des utilisateurs	1.2.3 2.5.3
Contrôle de l'application de la politique d'autorisation	1.1.1 2.2.3 2.8.2 2.8.3
Chiffrement des échanges	2.6.2 2.6.3
Cloisonnement des réseaux	2.4.5 2.5.4 2.6.1

SERVICES DE SECURITE (confidentialité)	REFERENCE PRINCIPE PSC
Contrôle du routage des accès sortants	2.4.5 2.5.4
Détection d'intrusion	2.5.4
Supervision des réseaux avec corrélation d'événements (détection, intrusion, filtrage)	2.4.5 2.5.7
Filtrage des flux	2.5.4
Plan de gestion des incidents (détection, traitement, investigation)	2.2.3 2.4.4
Contrôle de la télé-maintenance et de la télé-exploitation	1.2.4 2.5.4
Contrôle des accès informatiques depuis le réseau téléphonique	2.5.4
Plan de communication de crise	2.7
Plan de gestion des incidents (détection, traitement, investigation)	2.2.3 2.4.4
Protection anti-virale	2.4.3
Protection contre le rejeu et les doubles traitements des flux	2.6.2
Procédure d'habilitation du personnel technique	2.2.1 2.2.2
Contrôle d'accès physique	2.3.2
Supervision automatisée du respect de la politique d'autorisation	2.5
Sécurité physique des équipements (réseaux, serveurs…)	2.3.2

8.3.4. Services de preuve et de contrôle

SERVICES DE SECURITE (preuve et contrôle)	REFERENCE PRINCIPE PSC
Accusé de réception applicatif	2.6.2
Accusé de réception réseau	2.6.2
Signature électronique	2.6.2 2.8.1
Horodatage	2.6.2
Horodatage sécurisé	
Enregistrement et archivage du contrôle d'accès logique	2.5.7
Traçabilité des opérations d'administration	2.4.4 2.5.7
Traçabilité des opérations de maintenance applicative (modifications des programmes)	2.6.5
Traçabilité des opérations sensibles dans les applications	2.6.2
Traçabilité des opérations d'exploitation	2 .4

SERVICES DE SECURITE (preuve et contrôle)	**REFERENCE PRINCIPE PSC**
Gestion des preuves non informatiques	2.8.1
Archivage sécurisé des preuves électroniques	2.1.2 2.8.1
Authentification des personnes	2.5.2 2.5.4
Authentification des services	2.5.2
Authentification forte de personne et des services	2.5.1 2.5.2 2.5.4 2.5.5 2.5.6 2.8.1
Exploitation des traces pour la surveillance et le contrôle	2.4.4 2.5.7
Enregistrement et archivage selon la durée légale des adresses d'origine des accès réseaux	2.4.4
Enregistrement et archivage des traces du contrôle d'accès physique	2.3.1
Exploitation a posteriori des traces pour le contrôle et l'investigation	2.8
Investigation sur incident	2.8.1
Contractualisation des relations avec des tiers	1.2.4

8.4. Grille des niveaux de service (définition des niveaux de service)

NIVEAU de risque	DISPONIBILITE	INTEGRITE	CONFIDENTIALITE	PREUVE & CONTROLE
1 COURANT	**Interruption > à 1 journée** Une indisponibilité des informations est acceptée sous réserve qu'elle ne remette pas en cause le service fourni	**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	**Public** Les informations peuvent être lues par tous	**Faible** Les éléments d'auditabilité sont faibles et non immédiatement disponibles Exemple : journalisation d'accès
2 SENSIBLE	**Interruption < ou = 1 journée** Indisponibilité tolérée sous réserve qu'elle soit momentanée, signalée et sans conséquence pour le service fourni	**Signalement et correction** Perte tolérée si signalée et corrigée dans un délai suffisant pour ne pas avoir de conséquence grave sur le service fourni	**Restreint** Les informations sont diffusées ou accessibles par des populations identifiées et contrôlables	**Auditable** Les éléments de traçabilité des opérations existent et peuvent être rendus disponibles
3 MAJEUR (ou CRITIQUE)	**Interruption < ou = 1 / 2 journée** Les informations doivent toujours être fournies pour remplir le service attendu	**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	**Secret médical ou professionnel** Les informations sont protégées par le secret médical ou le secret professionnel et par la législation sur les données à caractère personnel et médical. Données nominatives non médicales Les informations sont protégées par la législation sur la protection des données nominatives	**Preuve interne** Fourniture d'une preuve opposable (mais contestable)
4 STRATE-GIQUE (ou VITAL)	**Interruption comprise entre 15' et 1h** Les informations doivent en permanence être accessibles et utilisables par tous les services concernés	**Certification a priori** Les informations sont certifiées intègres pendant toute leur durée de vie ou leur période de validité	**Haute protection** Le secret médical est renforcé Exemple : informations dont la prise de connaissance non autorisée entraîne nécessairement un préjudice pour la personne concernée (ex : certaines pathologies)	**Preuve externe** Fourniture d'une preuve incontestable

8.5. Grille de sélection des services

8.5.1. Services à mettre en œuvre par des procédures

Services	D				I				C				P			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Charte											X	X				
Contractualisation des relations avec les tiers														X	X	X
Contrat de maintenance	X	X	X	X												
Contrat de service (interne, externe) – fourniture de configurations de remplacement		X	X	X												
Contrôle d'accès physique		X	X	X							X	X				
Contrôle de la conformité de la configuration							X									
Contrôle de l'application de la politique d'autorisation											X	X				
Contrôle d'intégrité physique du câblage							X	X								
Exploitation a posteriori des traces pour le contrôle et l'investigation														X	X	X
Gestion de la documentation		X	X													
Gestion des preuves non informatiques														X	X	X
Habilitation des sous-traitants											X	X				
Investigation sur incident															X	X
Maintenance sécuritaire (patchs)			X	X												
Procédure de reprise sur incident			X	X												
Procédure d'habilitation du personnel technique			X	X		X	X	X			X	X				
Sensibilisation des utilisateurs							X	X			X	X				

Supervision des réseaux (procédures manuelles)		X														

8.5.2. Services mis en œuvre avec des mécanismes techniques de prévention/protection des configurations

Services	D				I				C				P			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Accusé de réception applicatif															X	X
Accusé de réception réseau														X	X	X
Accusé réception								X								
Activation de la procédure automatisée de roll-back pour la base de données								X								
Archivage sécurisé des preuves électroniques																X
Authentification des personnes						X	X			X	X				X	
Authentification des services							X				X				X	
Authentification forte des personnes								X				X				X
Authentification forte des services								X				X				X
Authentification mutuelle de l'émetteur et du destinataire d'un flux												X				
Automatisation de l'exploitation				X												
Chiffrement des échanges								X				X				
Cloisonnement des réseaux											X	X				
Confidentialité des données (chiffrement, anonymat)								X				X				
Contrôle automatisé de la conformité de la configuration								X								
Contrôle d'accès logique aux fonctions d'administration						X	X	X			X	X				

Services	D				I				C				P			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Contrôle d'accès logique (mise en œuvre du modèle complet de la PA)												X				
Contrôle d'accès logique (mise en œuvre du modèle intermédiaire ou complet de la PA)						X	X	X			X					
Contrôle d'accès logique (mise en œuvre du modèle simple ou intermédiaire de la PA)					X					X						
Contrôle de contenu			X	X			X	X			X	X				
Contrôle de la télé-maintenance et de la télé-exploitation											X	X				
Contrôle des accès aux réseaux informatiques depuis les réseaux téléphoniques											X	X				
Contrôle d'intégrité logique du réseau							X	X								
Contrôle d'intégrité physique du réseau								X								
Contrôle du routage des accès sortants											X	X				
Détection d'intrusion			X	X			X	X			X	X				
Disques à tolérance de pannes				X												
Enregistrement et archivage des traces du contrôle d'accès logique													X	X	X	X
Enregistrement et archivage des traces du contrôle d'accès physique														X	X	X
Enregistrement et archivage selon la durée légale des adresses d'origine des accès réseaux														X	X	X
Enregistrement redondant ou mirroring				X												
Filtrage des flux	X	X	X	X	X	X	X	X			X	X				

Services	D				I				C				P			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Gestion automatisée de la documentation				X												
Gestion de configuration			X	X			X	X								
Gestion des autorisations					X	X	X	X			X	X				
Gestion des profils					X	X	X	X			X	X				
Haute disponibilité (équilibrage de charges, doublement des configurations)				X												
Horodatage															X	
Horodatage sécurisé																X
Identification de l'origine des flux											X	X				
Journalisation des saisies							X	X								
Protection antivirale	X	X	X	X	X	X	X	X			X	X				
Protection contre le rejeu et contre le double traitement des flux								X			X	X				
Protection contre les modifications impropres ou illicites de configuration							X	X								
Reprise automatisée sur incidents				X			X	X								
Scellement (données sensibles, flux)								X								
Sécurité physique des équipements (réseaux, serveurs,..)	X	X	X	X		X	X	X			X	X				
Signature électronique								X								X
Supervision automatisée du respect de la politique d'autorisation												X				
Supervision des réseaux (alertes automatisées)			X				X	X			X					
Supervision des réseaux avec corrélation d'évènements				X				X				X				

Services	D				I				C				P			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
(détection intrusion, filtrage, …)																
Traçabilité des opérations d'administration															X	X
Traçabilité des opérations de maintenance applicative (modifications des programmes)															X	X
Traçabilité des opérations d'exploitation (production)															X	X
Traçabilité des opérations sensibles dans les applications														X	X	X

8.5.3. Plans (services regroupant procédures et mécanismes)

Services	D				I				C				P			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Plan de sauvegarde (de production, de recours)	X	X	X	X		X	X	X								
Plan de secours informatique et réseaux		X	X	X												
Plan de gestion des incidents (détection, traitement, investigation)		X	X	X		X	X	X			X	X				
Plan de communication de crise		X	X	X							X	X				

8.6. Présentation des services de sécurité

Accusé de réception applicatif

L'application qui traite les informations reçues délivre à l'émetteur des informations un accusé de réception logique. Cet accusé de réception se distingue de l'accusé de réception réseau : on entend par accusé de réception logique un message signifiant à l'émetteur des informations que celles-ci vont être traitées par l'application.

Archivage sécurisé des traces

Les traces enregistrées –traces du contrôle d'accès logique (réseaux et applications), éléments de preuve dans le cadre de la signature électronique, traces des opérations sensibles dans les applications – sont archivées de manière sécurisée (copie parallèle sur un support distant, copie sur un support non réinscriptible, contrôle d'accès logique pour la consultation des traces,…) afin d'éviter des destructions et des altérations involontaires ou malveillantes de traces.

Authentification des personnes

Action de vérifier l'identité déclarée d'une entité. L'authentification a pour but de vérifier l'identité dont une entité se réclame.

Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.

Il existe classiquement trois méthodes d'authentification permettant de prouver l'identité d'une personne :

- Authentification basée sur la connaissance d'un secret (ex. : mot de passe)
- Authentification basée sur la possession d'un objet (ex. : carte à puce, jeton).
- Authentification basée sur une caractéristique physique (ex. biométrie).

Authentification des services

Par authentification des services, on entend la vérification de l'identité d'un composant à l'origine du flux asynchrone ou de le demande d'ouverture du dialogue synchrone. Le composant peut être un serveur ou une application. Dans ce cas l'authentification est basée sur la possession d'un secret ou d'un objet.

Authentification forte des personnes

Vérification de l'identité basée sur des éléments de certification de l'identité utilisant des procédés cryptographiques. Cette définition est une « libre » traduction de la définition donnée dans la norme ISO/IEC 9594-8(E)« Authentication by means of cryptographically derived credentials ».

Authentification forte des services

Vérification de l'identité basée sur l'utilisation d' un algorithme cryptographique à clé publique (RSA par exemple)

Authentification mutuelle de l'émetteur et du destinataire du flux

Vérification, préalable à tout échange, de l'identité de l'émetteur et du destinataire des informations (en général, authentification forte)

Automatisation de l'exploitation

Mise en œuvre de logiciels spécifiques permettant d'automatiser l'ordonnancement des travaux d'exploitation et leur surveillance.

Chiffrement des échanges

Transformation cryptographique des données produisant un cryptogramme.

Processus par lequel des données en texte clair sont transformées pour cacher leur signification

Cloisonnement des réseaux

Le cloisonnement vise à protéger le système d'information, et aussi les sous-ensembles sensibles du système d'information, des accès illicites. Le cloisonnement peut être physique ou logique : dans le cas du cloisonnement logique, les mécanismes utilisés sont principalement les règles de routage, la mise en place de V-LAN, le contrôle des flux à l'aide de firewalls et de passerelles applicatives.

Enregistrement et archivage des traces du contrôle d'accès logique

Toute action du contrôle d'accès logique (accès autorisés et accès refusés) fait l'objet d'un enregistrement. Les informations enregistrées comprennent les informations nécessaires à une investigation a posteriori des demandes d'accès. Elles sont conservées pendant un délai correspondant aux exigences légales.

Contractualisation des relations avec les tiers

Contrat, établi en conformité avec le cadre juridique fourni par le GMSIH, régissant les activités, les fournitures, les obligations et les responsabilités dans le cadre de l'ouverture d'un SI à des tiers ou dans le cas d'externalisation d'activités. Ces contrats doivent intégrer les clauses d'application de la politique de sécurité ainsi que les règles de surveillance.

Contrat de maintenance

Contrat par lequel un fournisseur informatique ou télécommunication s'engage sur la fourniture de prestations de support, de maintenance corrective et évolutive des composants du système d'information.

Contrat de service (interne, externe) – fourniture de configurations de remplacement

Convention interne par laquelle une entité s'engage à fournir un service à une autre entité de la même organisation, en précisant les modalités de fourniture de ce service.

Contrat externe par lequel un fournisseur informatique ou télécommunication s'engage sur la fourniture d'un service, les modalités de fourniture du service, les pénalités, les recours et indicateurs associés à l'exécution du contrat.

Contrôle conformité configuration

Ensemble des procédures et de tests visant à vérifier la conformité des configurations à un référentiel (paramétrage, version mise en production,…)

Contrôle automatisé de la conformité d'une configuration

Ensemble de procédures automatisées de contrôle de conformité d'une configuration.

Contrôle d'accès logique aux applications et données

Ensemble des moyens logiciels garantissant que seules les entités autorisées peuvent accéder aux ressources d'un système d'information automatisé, et seulement d'une manière autorisée.

Les spécifications du contrôle d'accès logique doivent répondre aux modèles de la Politique d'Autorisation du GMSIH.

Contrôle d'accès logique aux fonctions d'administration

Ensemble des moyens logiciels garantissant que seules les entités autorisées peuvent accéder aux fonctions d'administration d'un système informatique, et seulement d'une manière autorisée.

Contrôle d'accès physique

Dispositif humain, matériel ou matériel et logiciel garantissant que seules les personnes autorisées peuvent accéder aux installations protégées (entrée contrôlée par un gardien, ouverture d'une porte ou d'un sas sur la base d'une clé physique ou logique – code, carte, empreinte,..)

Contrôle d'intégrité physique du câblage

Procédure d'examen périodique des chemins de câble, baies de brassage et autres éléments physiques du câblage pour en vérifier l'intégrité.

Contrôle d'intégrité logique du réseau

Mécanisme permettant de détecter automatiquement les ruptures logiques d'intégrité du réseau (conflits d'adresses IP, passage de cartes réseau en mode promiscuous, etc.).

Contrôle de la télé-maintenance et de la télé-exploitation

Mise en œuvre de mécanismes (rappel automatique, ouverture de port, établissement d'un VPN,…) permettant de contrôler les accès au système d'information par des tiers externes autorisés à réaliser des opérations sensibles telles que la maintenance ou l'exploitation à distance.

Contrôle des accès informatiques depuis le réseau téléphonique

Ensembles des mesures techniques garantissant que seules les entités et les flux autorisés peuvent accéder aux ressources du système informatique depuis le réseau téléphonique.

Contrôle du routage des accès sortants

Contrôle de l'autorisation d'un flux à sortir du LAN vers les réseaux externes.

Détection d'intrusion logique

Service de détection d'intrusion sur un réseau réalisé par observation automatisée des évènements et des traces des évènements (demande de connexion, répétition d'actions,…), comparaison avec des bases d'attaque et corrélation d'évènements.

Enregistrement redondant ou mirroring

Enregistrement simultané en temps réel ou en temps très légèrement différé des données sur deux supports physiques distincts.

Exploitation a posteriori des traces pour le contrôle et l'investigation

Procédures opérationnelles de contrôle des traces des dispositifs de sécurité (authentifications, accès logiques et réseaux, détection d'intrusion,…) en vue de la supervision de l'application de la politique de sécurité. L'investigation fait l'objet de procédures spécifiques placées dans le cadre du plan de gestion des incidents.

Filtrage des flux

Ensemble des mesures techniques permettant de contrôler les communications, les flux entre sources et destinataires par le biais de règles de restriction des accès configurées au niveau des équipements réseaux : règles de filtrage sur firewall, règles de routage (interdiction de router une @IP sur le LAN…)

Enregistrement et archivage des traces du contrôle d'accès logique

Activation de la fonction d'enregistrement des évènements du contrôle d'accès logique, et utilisation de supports assurant la conservation de ces enregistrements selon une durée et dans des conditions de sécurité déterminées.

Enregistrement et archivage des traces du contrôle d'accès physique

Lorsque le mécanisme de contrôle d'accès physique le permet, enregistrement des évènements du contrôle d'accès physique et conservation des enregistrements selon une durée et dans des conditions déterminées.

Gestion de configuration

Ensemble de procédures, supportée ou non dans un gestionnaire de configuration automatisé, garantissant qu'à chaque étape du cycle de vie du logiciel (développement, recette technique, recette fonctionnelle, diffusion, mise en production, maintenance), le logiciel est intégré dans les espaces physique et logique correspondants et soumis à un référentiel spécifique.

Gestion de la documentation

Ensemble de procédures encadrant la production et la mise à jour de la documentation des ressources du système d'information, la conservation de la documentation pour chaque version de la ressource, et les conditions de destruction de la documentation.

Gestion automatisée de la documentation

Outil logiciel permettant de gérer les différentes versions des logiciels à chaque étape du cycle de vie.

Gestion des autorisations

Ensemble de procédures organisationnelles et techniques d'attribution à une entité des droits d'accès, complet ou restreint, à une ressource. La Politique d' Autorisation publiée par le GMSIH indique les différents modèles organisationnels pour cette gestion.

Plan de gestion des incidents (détection, traitement, investigation)

Enchaînement d'activités procédurales et techniques visant à gérer les incidents de sécurité de toute nature (intrusion logique, perte d'intégrité,…)

Gestion des preuves non informatiques

Gestion des moyens de preuves sur support magnétique (enregistrements vidéo,…) et sur support papier : télex, fax,…

Gestion des profils

Ensemble des procédures organisationnelles et technique permettant de vérifier, mettre à jour, résilier les « profils ».

Pour chaque utilisateur individuel, ou chaque groupe particulier d'utilisateurs, regroupés par exemple par projet, on établit un "profil", comportant :

- une identification (nom, fonction, organisation, etc.),
- une matrice d'accès et habilitation propre à cet utilisateur ; en fonction du type et de la classe des données

Reprise automatisée sur incident

Ensembles des automatismes techniques permettant de reprendre les activités interrompues par un incident (machine, logiciel, base de données,…)

Haute disponibilité

Service obtenu par le doublement des configurations et des chemins d'accès réseaux, et par un mécanisme d'équilibrage de charges (en nombre de connexions acceptées) sur les configurations concernées.

Habilitation des sous-traitants

Procédure d'habilitation du personnel informatique et télécommunications des sociétés sous-traitantes : déclaration des identités et des profils, attribution d'autorisations dans le système d'information.

Horodatage

(« time-stamping service ») Apposition d'un « tampon » électronique de date et heure sur un événement donné (date et heure de connexion, de réception d'un message,…), élaboré à partir d'une « horloge » dont la fiabilité est contractuellement acceptée par les parties de l'échange. Ce « tampon » fait partie des éléments constitutifs de la trace de l'évènement.

Horodatage sécurisé

Service d'horodatage délivré par une autorité d'horodatage (tierce partie de confiance pour l'horodatage).

Identification de l'origine du flux

Identification et enregistrement de l'adresse IP à l'origine du flux.

Investigation sur incident

Mise en œuvre de techniques d'investigation en cas d'incident portant atteinte à la sécurité du système d'information : analyse des traces, observations d'évènements,…

Journalisation des saisies

Enregistrement au fil de l'eau des éléments relatifs aux saisies de manière à reconstituer le fichier ou la base de données après incident (destruction, altération).

Maintenance sécuritaire (patchs)

Procédure d'intégration systématique des correctifs de sécurité publiés par le fournisseur d'un système d'exploitation, d'un logiciel, d'un équipement réseau

Plan de sauvegarde (de production, de recours)

Définition et mise en œuvre des sauvegardes selon les périodicités définies pour chaque application ou système (prise en compte de la criticité de l'application ou du système) ; les sauvegardes de recours sont stockées dans un local distant des locaux de production ; la description du plan de sauvegarde est donnée dans la Politique de Sécurité Cadre

Plan de secours informatique et réseaux

Ensemble de procédures permettant de restaurer le système informatique et réseaux sur un site de secours suite à un sinistre affectant tout ou partie des systèmes d'information.

Procédure d'habilitation du personnel technique

Procédure à suivre lors de toute arrivée d'un nouvel agent dans un service de développement, d'administration systèmes et réseaux, de production informatique.

Procédure de reprise sur incident

Procédure manuelle permettant de reprendre les activités interrompues par un incident (machine, logiciel, base de données,…)

Protection antivirale

Ensemble des moyens techniques et organisationnels permettant de détecter les virus, d'empêcher les infections virales, éventuellement de les éradiquer, et de décontaminer les équipements atteints par l'attaque virale.

Protection contre le rejeu et contre le double traitement des flux

Prévention des doubles prises en compte d'un même flux par un contrôle de séquencement et de contenu ; prévention du rejeu en authentification, par l'introduction d'une donnée aléatoire et de données variables dans le dialogue d'authentification

Protection contre les modifications impropres ou illicites de configuration

Procédure ou mécanisme permettant de détecter les modifications non autorisées de configurations informatiques et réseaux

Protection physique des équipements

Dispositifs de protection physique visant à protéger l'intégrité des équipements et la confidentialité des données hébergées par cet équipement (contrôle d'accès physique, protection contre l'incendie et le dégât des eaux,…)

Scellement (données sensibles, flux)

Fonction de chiffrement produisant un cryptogramme à partir duquel les données originelles ne peuvent être reconstituées (fonction dite à sens unique).

Sécurité physique des équipements (réseaux, serveurs…)

Dispositifs permettant d'assurer la protection physique des matériels, soit en protégeant les locaux, soit directement le matériel. Ces dispositifs permettent de lutter contre les agressions involontaires (accidents, erreurs) et malveillantes.

Il s'agit classiquement de la protection contre l'incendie, les dégâts des eaux, les agressions physiques, la sécurité électrique…

Sensibilisation des utilisateurs

Actions de sensibilisation des personnels au respect du secret professionnel lors de l'utilisation des fonctions et des informations contenues dans le système d'information automatisé. La Charte de sécurité est un autre vecteur de sensibilisation. Lorsque la Charte est annexée au règlement intérieur, ses

dispositions deviennent opposables à l'utilisateur. L'utilisateur externe doit être également sensibilisé (professionnel de santé,..)

Signature électronique

La signature électronique « consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel il s 'attache » (loi du 13 mars 2002). L'algorithme utilisé est un algorithme asymétrique (RSA) : la clé publique est stockée dans un certificat délivré par une autorité de certification.

Supervision automatisée du respect de la politique d'autorisation

L'administrateur ou le RSSI sont avertis dès que la politique d'autorisation n'est pas respectée (via la messagerie ou une console d'administration).

Supervision des réseaux (procédures manuelles)

La supervision des réseaux consiste à surveiller l'activité (trafic, événements de sécurité…) sur chacun des éléments du réseau : routeurs, éléments actifs, firewall…

Supervision des réseaux (procédures automatisées)

La supervision automatisée des réseaux est l'utilisation de logiciels et mécanismes surveillant automatiquement l'activité des réseaux et déclenchant des alertes sur événements programmés à l'avance (dépassement d'un seuil, événement suspect…).

Traçabilité des opérations d'administration

La traçabilité des opérations d'administration consiste à journaliser l'ensemble des actions menées par les administrateurs du système considéré (ex : ouverture d'un compte administrateur, création/suppression de comptes, modification des droits d'accès, accès aux journaux de sécurité…).

Traçabilité des opérations sensibles dans les applications

L'application enregistre tous les éléments pertinents (a minima identité de l'acteur, données concernées, actions réalisées par l'acteur) pour les opérations sensibles de l'application. Les traces peuvent ensuite être conservées de manière centralisée ou par application.

8.7. Couverture fonctionnelle de l'analyse des risques pour les domaines de sécurité des SIH par rapport aux scenarii de la norme ENV 13606-4

8.7.1. Nature des flux analysés pour les Profils Fonctionnels de Sécurité

Dans l'analyse de risques réalisée pour l'élaboration des Profils Fonctionnels de Sécurité, on s'est attaché à évaluer la sensibilité en Disponibilité, Intégrité, Confidentialité, Preuve et Contrôle des flux d'informations nécessaires aux activités menées par les différents acteurs du système d'information.

Par exemple dans un établissement travaillant au sein d'un réseau de santé, pour les activités définies dans le cas représentatif, les flux sont les suivants :

Flux

Ressource	D	I	C	P
Convocation à un rendez-vous	1	2	4	2
Demande d'inscription	1	2	4	1
Evaluation	1	2	2	1
Inscription du patient	2	3	4	2
Sortie	1	3	4	2
Sortie de prestation	1	3	4	2
Consultation ou téléchargement d'une extraction du dossier	3	3	4	2

Ou encore, dans le cadre du système d'information interne d'un établissement (SIH) :

Flux de données

Ressource	D	I	C	P
Admission générale	2	2	3	2
Admission service	3	4	3	2
Admission urgences	4	4	3	2
Demande de prestation	3	3	3	3
PMSI	2	2	3	2
Prise de rendez-vous	2	1	3	2
Prise en charge médicale	4	4	3	3
Réalisation de prestation	3	4	3	3

Réception de demande de prestation	3	3	3	3
Ressource	**D**	**I**	**C**	**P**
Réponse suite à prestation	2	4	3	3
Sortie de l'établissement	1	2	3	2
Sortie de service	3	4	3	3
Vigilance (transmission des fiches)	2	2	3	2

Flux d'administration

Ressource	**D**	**I**	**C**	**P**
Administration système	3	4	4	2
Télémaintenance	3	4	4	2

Le périmètre des PFS couvre principalement les messages relatifs à la prise en charge administrative et médicale du patient (transmission de données patients).

8.7.2. Emetteur et destinataire des flux

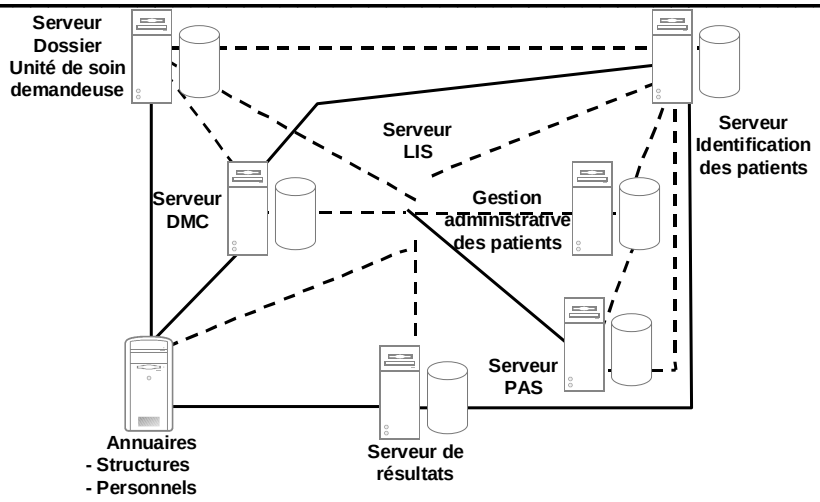
La description des activités métiers, ainsi que les représentations des architectures, permettent de situer l'émetteur et le destinataire du flux.

Par exemple :

Réponse prestation – labo

La réponse de prestation est le retour au demandeur des résultats d'analyse. Lors que l'établissement en est équipé, ces résultats sont publiés dans le serveur de résultats.

Dans certains cas, ils pourront aussi être transmis au serveur de dossier commun ou au serveur de dossier de l'unité de soin demandeuse.



8.7.3. Les scenarii la 13606-4 et leur correspondance dans l'analyse des risques menée pour les PFS

Les scenarii de la 13606-4 impliquant un échange entre deux parties

Scenarii de la 13606-4	Flux Etude GMSIH
Scenarii de la 13606-4 impliquant deux parties dans l'échange de messages	
Transfert du dossier médical d'une structure à une autre, à l'initiative de la structure actuellement responsable, lorsque le patient change de structure pour la délivrance des soins	Pas de cas de transfert définitif de dossier médical d'une structure à une autre (exemple anglais de changement de généraliste non étudié ici car hors champ)
Transfert du dossier médical d'une structure à une autre, à l'initiative de la future structure responsable, lorsque le patient change de structure pour la délivrance des soins	Pas de cas de transfert définitif de dossier médical d'une structure à une autre (exemple anglais de changement de généraliste non étudié ici car hors champ)
Demande d'informations du dossier médical par une structure soignant le patient de manière temporaire (exemple, le service d'urgence)	Demande au réseau de santé par l'hôpital d'un extrait du dossier du patient, ou consultation en ligne par le praticien de l'établissement participant au réseau (PFS Réseau de santé)
Envoi par la structure soignant le patient d'informations à une structure soignant temporairement le patient	Envoi des résultats de la prestation par l'établissement B ayant réalisé une prestation pour un patient de l'établissement A (PFS Coopération inter – établissements)
Envoi de messages dans le cadre d'une prestation spécifique déléguée par la structure responsable du patient à une autre structure	Envoi des informations et de la demande de prestation d'un patient de l'établissement A vers un établissement B pour la réalisation d'une prestation (PFS Coopération inter – établissements)

Scenarii de la 13606-4	Flux Etude GMSIH
Scenarii de la 13606-4 impliquant deux parties dans l'échange de messages	
Envoi de messages dans le cadre de demandes itératives de prestations spécifiques déléguée par la structure responsable du patient à une autre structure	Processus itératif de demandes /réalisations/ réponses de prestations dans tous les PFS concernés

Les scenarii de la 13606-4 impliquant une tierce partie de confiance dans l'échange de messages

Scenarii de la 13606-4	Flux Etude GMSIH
Scenarii de la 13606-4 impliquant une tierce partie de confiance dans l'échange de messages	
Une structure A sait qu'une autre structure va demander des informations médicales, mais ne connaît pas l'identité de cette autre structure ; Une structure C agit comme un hébergeur de dossiers de santé informatisés	Ce cas n'a pas été traité pour les raisons suivantes : 1) le cas où le patient est son propre hébergeur de dossier médical informatisé est très peu répandu : le patient est aujourd'hui une entité qui autorise ou refuse la mise à disposition de ses informations à des professionnels de santé 2) le cas où le réseau de santé n'a pas de système d'information en propre, et où un « régulateur » traite les demandes d'envoi d'extraits de dossiers n'a pas été traité dans l'étude 3) le cas d'un hébergeur de dossiers médicaux au sens des textes n'a pas été étudié faute de recul sur la question d'une part, et d'autre part de texte régissant les obligations liées à cette activité

Scenarii de la 13606-4	Flux Etude GMSIH
Scenarii de la 13606-4 impliquant une tierce partie de confiance dans l'échange de messages	
La structure C agit comme un centre médical qui reçoit des demandes de prestations de la part d'une structure A, gère la répartition des réalisations de prestations sur des structures B, et gère les échanges d'informations médicales associées ; par exemple les informations médicales d'un touriste blessé dans un pays étranger sont rapatriées par l'assureur à la structure de soins du pays d'origine; ou encore un patient cardiaque suivi par un généraliste doit être hospitalisé d'urgence : l'hospitalisation est décidée par la structure C qui envoie le patient à l'hôpital régional (structure B) avec les éléments d'informations nécessaires	Non étudié, car le champ de l'étude « Services de Sécurité » concerne le domaine de sécurité de l'établissement de santé, en relation avec d'autres domaines de sécurité (vision « hospitalo-centrée »
Les procédures d'accréditation, et de vérification de l'accréditation de la tierce partie sont hors champ de la norme	Traité dans l'étude pour les aspects de mise en œuvre de mécanismes de sécurité
L'authenticité de l'origine par la signature électronique, par exemple, est hors champ de la norme	Traité dans l'étude

8.7.4. Mise en regard des natures de flux étudiés

La 13606-4 étudie les flux sous la forme de cinématique d'échanges unitaires : par exemple, lorsque la structure B veut obtenir les informations du patient détenues par la structure A, plusieurs messages sont échangés :

- Message de requête envoyé par la structure B
- Message de refus d'envoi du dossier envoyé par la structure A
- Message d'envoi du dossier par la structure A
- Message d'envoi de mise à jour du dossier détenu par la structure A envoyé par B

L'échange peut être réalisé dans différents contextes de soins : sa structure est toujours identique, et il comprend trois messages génériques principaux : le message de requête du dossier patient, le message de fourniture du dossier, le message de notification (c'est-à-dire de refus de la communication du dossier).

Dans le cadre de l'étude menée au GMSIH, l'analyse des risques est basée sur les principes suivants :

- les flux sont des ressources nécessaires à la réalisation de l'activité,
- ils ont la même sensibilité que toutes les autres informations nécessaires à la réalisation de l'activité : seules les vulnérabilités du canal utilisé peuvent augmenter le besoin de sécurité du flux

par rapport à celui des autres ressources de l'activité (par exemple, le besoin de protection en confidentialité des flux d'information médicales concernant le patient).

L'étude du GMSIH permet d'aborder plus finement la sécurité, dans la mesure où tous les critères (D,I,C,P) sont évalués et justifiés par les situations métiers des cas représentatifs de domaines de sécurité : c'est ce qui permettra au RSSI de justifier la mise en œuvre des services de sécurité.

Le but des scenarii de la 13606-4 est différent : ils concernent principalement des situations génériques, ainsi que les critères de confidentialité et de preuve et contrôle et viennent illustrer les applications du schéma normalisé de communication des données de santé.

8.7.5. La mise en œuvre des services de sécurité

Les services de sécurité correspondant aux flux d'informations médicales échangées sont traités dans les profils fonctionnels de sécurité : on définit, pour chaque flux de cas représentatifs de domaines de sécurité, quels sont les services de sécurité à mettre en selon leur besoin de sécurité. Ces services sont mis en œuvre par des procédures et contrats, des mécanismes techniques ou des plans.

Les mécanismes techniques – authentification mutuelle forte de l'émetteur et du destinataire, signature électronique, vérification du certificat, … - seront traités dans l'étude des solutions.

8.8. Catalogue des sinistres potentiels évalués pour l'établissement des profils fonctionnels de sécurité

Catalogue de sinistres potentiels	
Cas : SIH	**Processus : Hospitalisation**
Activités	**Nature du risque**
Prise de rendez-vous	• Indisponibilité de la prise de RV pendant 1 journée (indiquer le délai maximal d'interruption toléré – DMIA-) • Erreur dans la prise de RV (sur l'identité du patient, sur la disponibilité du médecin, sur l'horaire) • Prise de RV confidentielle (VIP, personnel) rendue publique • Absence de preuve d'une prise de RV en cas de litige
Admission générale	• Impossibilité de procéder à l'admission générale du patient • Erreur d'identification du patient lors de son admission • Rupture de la confidentialité de l'admission d'un VIP ou d'un membre du personnel • Absence de trace de l'admission générale du patient
Admission service	• Impossibilité de procéder à l'admission au niveau du service ? ?: (indisponibilité de l'application de gestion du dossier médical, indisponibilité de l'application de production des soins) • Erreur d'identification du patient lors de son admission • Rupture de la confidentialité de l'admission d'un VIP ou d'un membre du personnel • Absence de trace de l'admission générale du patient

Catalogue de sinistres potentiels

Cas : SIH	**Processus : Hospitalisation**

Activités	**Nature du risque**
PEC médicale	• Impossibilité de prendre en charge médicalement les patients (manque de ressources) pendant plus de 24 heures • Erreur dans la dispensation des soins et des médicaments • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité des actes effectués • Absence de preuve des actes dispensés
Demande de prestation	• Impossibilité d'effectuer la demande de prestation pendant 24 h (donner le DMIA) • Erreur dans la demande de prestation • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la demande de prestation • Absence de preuve de la demande de prestation
Réception demande	• Impossibilité de réceptionner la demande de prestation pendant 24 h (donner le DMIA) • Non rectification de l'erreur dans la demande de prestation • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la réception de demande ; rectification non tracée • Absence de preuve de la réception de la demande, absence de preuve de la rectification

Catalogue de sinistres potentiels

Cas : SIH	**Processus : Hospitalisation**

Activités	**Nature du risque**
Réalisation prestation (imagerie)	• Impossibilité de réaliser la prestation pendant 24 h (donner le DMIA) • Erreur d'identification du patient • Erreurs dans la réalisation de la prestation : prestation non demandée, erreur de réalisation de la prestation demandée • Non respect du secret médical • Absence de traçabilité de la réalisation (qui, quoi) • Absence de preuve de la réalisation (qui, quoi, perte de l'image et du résultat)
Réponse prestation (imagerie)	• Impossibilité d'obtenir le résultat pendant (donner le DMIA) • Erreur d'identification du patient • Erreur dans le résultat de la prestation • Omission d'un élément dans la transmission du résultat • Non respect du secret médical • Absence de traçabilité de la réponse de prestation • Absence de preuve de la transmission de la réponse de prestation

Catalogue de sinistres potentiels

Cas : SIH	**Processus : Hospitalisation**
Activités	**Nature du risque**
Réalisation prestation (labo)	• Impossibilité de réaliser la prestation pendant 24 h (donner le DMIA) • Erreurs dans la réalisation de la prestation : prestation non demandée, erreur de réalisation de la prestation demandée • Non réalisation de la prestation (absence de résultat) • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la réalisation (qui, quoi) • Absence de preuve de la réalisation (qui, quoi, perte de l'image et du résultat)
Réponse prestation (labo)	• Impossibilité d'obtenir le résultat pendant (donner le DMIA) • Erreur dans le résultat de la prestation • Omission d'un élément dans la transmission du résultat • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la réponse de prestation • Absence de preuve de la transmission de la réponse de prestation

Catalogue de sinistres potentiels

Cas : SIH	**Processus : Hospitalisation**
Activités	**Nature du risque**
Réception réponse	• Impossibilité de communiquer la réponse de prestation à l'entité à l'origine de la demande de prestation pendant (donner le DMIA) • Erreur lors de la réception de la réponse • Eléments manquant lors de la réception • Erreur d'identification du patient • Non respect du secret médical • Absence de la traçabilité de la réception • Absence de preuve de la réception de la réponse
Sortie service (mutation)	• Impossibilité de réaliser la sortie de service pendant 24 h (donner le DMIA) • Erreur dans la mutation de service • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la mutation • Absence de preuve de la mutation
Sortie établissement	• Impossibilité de réaliser la sortie de l'établissement pendant 24 h (donner le DMIA) • Erreur d'identification du patient • Erreur dans la mutation de service • Non respect du secret médical • Absence de traçabilité de la mutation • Absence de preuve de la mutation

Catalogue de sinistres potentiels

Cas : SIH	**Processus : Hospitalisation**
Activités	**Nature du risque**
Demande PEC réseau de santé	• Impossibilité de faire prendre en charge le patient sortant par le réseau de santé pendant 24 h (donner le DMIA) • Erreur d'identification du patient • Erreur d' « adressage » de la prise en charge (erreur choix réseau de santé destinataire) • Non respect du secret médical • Absence de traçabilité de la demande de prise en charge par le réseau • Absence de preuve de la demande de prise en charge par le réseau
PMSI	• Indisponibilité des RUM et du RSA • Inexactitude des données • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité des opérations PMSI

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Consultation externe**

Activités	Nature du risque
Prise de rendez-vous	• Indisponibilité de la prise de RV pendant 1 journée (indiquer le délai maximal d'interruption toléré) • Erreur dans la prise de RV (sur l'identité du patient, sur la disponibilité du médecin, sur l'horaire) • Prise de RV confidentielle (VIP, personnel) rendue publique • Absence de trace de la prise de RV • Absence de preuve d'une prise de RV en cas de litige
Admission générale	• Impossibilité de procéder à l'admission générale du patient • Erreur d'identification du patient lors de son admission • Rupture de la confidentialité de l'admission d'un VIP ou d'un membre du personnel • Absence de trace de l'admission générale du patient
Admission service	• Impossibilité de procéder à l'admission au niveau du service ? ?: (indisponibilité de l'application de gestion du dossier médical, indisponibilité de l'application de production des soins) • Erreur d'identification du patient lors de son admission • Rupture de la confidentialité de l'admission d'un VIP ou d'un membre du personnel • Absence de trace de l'admission générale du patient

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Consultation externe**

Activités	Nature du risque
PEC médicale	• Impossibilité de prendre en charge médicalement les patients (manque de ressources) pendant plus de 24 heures • Erreur dans la dispensation des soins et des médicaments • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité des actes effectués • Absence de preuve des actes dispensés
Demande de prestation	• Impossibilité d'effectuer la demande de prestation pendant 24 h (donner le DMIA) • Erreur dans la demande de prestation • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la demande de prestation • Absence de preuve de la demande de prestation
Réception demande	• Impossibilité de réceptionner la demande de prestation pendant 24 h (donner le DMIA) • Non rectification de l'erreur dans la demande de prestation • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la réception de demande ; rectification non tracée • Absence de preuve de la réception de la demande, absence de preuve de la rectification

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Consultation externe**

Activités	**Nature du risque**
Réalisation prestation (imagerie)	• Impossibilité de réaliser la prestation pendant 24 h (donner le DMIA) • Erreur d'identification du patient • Erreurs dans la réalisation de la prestation : prestation non demandée, erreur de réalisation de la prestation demandée • Non respect du secret médical • Absence de traçabilité de la réalisation (qui, quoi) • Absence de preuve de la réalisation (qui, quoi, perte de l'image et du résultat)
Réponse prestation (imagerie)	• Impossibilité d'obtenir le résultat pendant (donner le DMIA) • Erreur d'identification du patient • Erreur dans le résultat de la prestation • Omission d'un élément dans la transmission du résultat • Non respect du secret médical • Absence de traçabilité de la réponse de prestation • Absence de preuve de la transmission de la réponse de prestation

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Consultation externe**

Activités	**Nature du risque**
Réalisation prestation (labo)	• Impossibilité de réaliser la prestation pendant 24 h (donner le DMIA) • Erreurs dans la réalisation de la prestation : prestation non demandée, erreur de réalisation de la prestation demandée • Non réalisation de la prestation (absence de résultat) • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la réalisation (qui, quoi) • Absence de preuve de la réalisation (qui, quoi, perte de l'image et du résultat)
Réponse prestation (labo)	• Impossibilité d'obtenir le résultat pendant (donner le DMIA) • Erreur dans le résultat de la prestation • Omission d'un élément dans la transmission du résultat • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la réponse de prestation • Absence de preuve de la transmission de la réponse de prestation

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Consultation externe**

Activités	**Nature du risque**
Réception réponse	• Impossibilité de communiquer la réponse de prestation à l'entité à l'origine de la demande de prestation pendant (donner le DMIA) • Erreur lors de la réception de la réponse • Eléments manquant lors de la réception • Erreur d'identification du patient • Non respect du secret médical • Absence de la traçabilité de la réception • Absence de preuve de la réception de la réponse
Sortie service (mutation)	• Impossibilité de réaliser la sortie de service pendant 24 h (donner le DMIA) • Erreur dans la mutation de service • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la mutation • Absence de preuve de la mutation
Sortie établissement	• Impossibilité de réaliser la sortie de l'établissement pendant 24 h (donner le DMIA) • Erreur d'identification du patient • Erreur dans la mutation de service • Non respect du secret médical • Absence de traçabilité de la mutation • Absence de preuve de la mutation

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Consultation externe**

Activités	**Nature du risque**
Demande PEC réseau de santé	• Impossibilité de faire prendre en charge le patient sortant par le réseau de santé pendant 24 h (donner le DMIA) • Erreur d'identification du patient • Erreur d' « adressage » de la prise en charge (réseau de santé inadéquat) • Non respect du secret médical • Absence de traçabilité de la demande de prise en charge par le réseau • Absence de preuve de la demande de prise en charge par le réseau

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Urgences**

Activités	Nature du risque
Admission service	• Impossibilité de procéder à l'admission au niveau du service ? ?: (indisponibilité de l'application de gestion du dossier médical, indisponibilité de l'application de production des soins) • Erreur d'identification du patient lors de son admission • Rupture de la confidentialité de l'admission d'un VIP ou d'un membre du personnel • Absence de trace de l'admission générale du patient
PEC médicale	• Impossibilité de prendre en charge médicalement les patients (manque de ressources) pendant plus de 24 heures (donner le DMIA) • Erreur dans la dispensation des soins et des médicaments • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité des actes effectués • Absence de preuve des actes dispensés
Demande de prestation	• Impossibilité d'effectuer la demande de prestation pendant 24 h (donner le DMIA) • Erreur dans la demande de prestation • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la demande de prestation • Absence de preuve de la demande de prestation

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Urgences**

Activités	**Nature du risque**
Réception demande	• Impossibilité de réceptionner la demande de prestation pendant 24 h (donner le DMIA) • Non rectification de l'erreur dans la demande de prestation • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la réception de demande ; rectification non tracée • Absence de preuve de la réception de la demande, absence de preuve de la rectification
Réalisation prestation (imagerie)	• Impossibilité de réaliser la prestation pendant 24 h (donner le DMIA) • Erreur d'identification du patient • Erreurs dans la réalisation de la prestation : prestation non demandée, erreur de réalisation de la prestation demandée • Non respect du secret médical • Absence de traçabilité de la réalisation (qui, quoi) • Absence de preuve de la réalisation (qui, quoi, perte de l'image et du résultat)

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Urgences**

Activités	**Nature du risque**
Réponse prestation (imagerie)	• Impossibilité d'obtenir le résultat pendant (donner le DMIA) • Erreur d'identification du patient • Erreur dans le résultat de la prestation • Omission d'un élément dans la transmission du résultat • Non respect du secret médical • Absence de traçabilité de la réponse de prestation • Absence de preuve de la transmission de la réponse de prestation
Réalisation prestation (labo)	• Impossibilité de réaliser la prestation pendant 24 h (donner le DMIA) • Erreurs dans la réalisation de la prestation : prestation non demandée, erreur de réalisation de la prestation demandée • Non réalisation de la prestation (absence de résultat) • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la réalisation (qui, quoi) • Absence de preuve de la réalisation (qui, quoi, perte de l'image et du résultat)

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Urgences**

Activités	**Nature du risque**
Réponse prestation (labo)	• Impossibilité d'obtenir le résultat pendant (donner le DMIA) • Erreur dans le résultat de la prestation • Omission d'un élément dans la transmission du résultat • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la réponse de prestation • Absence de preuve de la transmission de la réponse de prestation
Réception réponse	• Impossibilité de communiquer la réponse de prestation à l'entité à l'origine de la demande de prestation pendant (donner le DMIA) • Erreur lors de la réception de la réponse • Eléments manquant lors de la réception • Erreur d'identification du patient • Non respect du secret médical • Absence de la traçabilité de la réception • Absence de preuve de la réception de la réponse

Catalogue des sinistres potentiels	
Cas : SIH	**Processus : Urgences**

Activités	**Nature du risque**
Sortie service (mutation)	• Impossibilité de réaliser la sortie de service pendant 24 h (donner le DMIA) • Erreur dans la mutation de service • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité de la mutation • Absence de preuve de la mutation
Sortie établissement	• Impossibilité de réaliser la sortie de l'établissement pendant 24 h (donner le DMIA) • Erreur d'identification du patient • Erreur dans la mutation de service • Non respect du secret médical • Absence de traçabilité de la mutation • Absence de preuve de la mutation
PMSI	• Indisponibilité des RUM et du RSA • Inexactitude des données • Erreur d'identification du patient • Non respect du secret médical • Absence de traçabilité des opérations PMSI

Catalogue des sinistres potentiels

Cas : Réseau de santé	**Processus : Inscription du patient**

Activités	**Nature du risque**
Demande inscription	• Impossibilité de demander l'inscription d' un patient pendant 1 journée (indiquer le délai maximal d'interruption toléré) • Erreur dans la demande d'inscription (sur l'identité du patient, sur la pathologie) • Demande d'inscription confidentielle (VIP, personnel, mineur, conjoint,…) rendue publique • Absence de trace de la demande • Absence de preuve de la demande en cas de litige
Inscription	• Impossibilité d'inscrire un patient pendant 1 journée (indiquer le délai maximal d'interruption toléré) • Erreur dans l'inscription (sur l'identité du patient, sur la pathologie) • Prise d'inscription confidentielle (VIP, personnel, mineur, conjoint,…) rendue publique • Absence de trace de l'inscription • Absence de preuve de l'inscription en cas de litige
Sortie du réseau de santé	• Impossibilité de réaliser la sortie du réseau pour ce patient pendant 24 h (donner le DMIA) • Erreur d'identification du patient pour sa sortie • Procédure de sortie du réseau rendue publique (VIP, personnel, mineur, conjoint,…) • Absence de trace de la sortie • Absence de preuve de la sortie en cas de litige

Catalogue des sinistres potentiels

Cas : Réseau de santé	**Processus : Prise en charge du patient**

Activités	**Nature du risque**
Demande de rendez-vous	• Indisponibilité de la prise de RV pendant 1 journée (indiquer le délai maximal d'interruption toléré -DMIA) • Erreur dans la prise de RV (sur l'identité du patient, sur la disponibilité du médecin, sur l'horaire) • Prise de RV confidentielle (VIP, personnel) rendue publique • Absence de trace de la prise de RV • Absence de preuve d'une prise de RV en cas de litige
Sortie de prestation	• Impossibilité de communiquer les résultats de prestation au système d'(indiquer le DMIA) • Erreur dans la communication des résultats et la mise à jour du dossier (erreur d'identification du patient, erreur de résultat) • Non respect du secret médical • Absence de traçabilité des prestations • Absence de preuve des prestations

Catalogue des sinistres potentiels

Cas : Réseau de santé	**Processus : Evaluation**

Activités	**Nature du risque**
Recueil des indicateurs	• Indisponibilité des indicateurs (indiquer le délai maximal d'interruption toléré -DMIA) • Erreur dans les indicateurs • Indicateur contenant des données médicales à caractère personnel • Absence de trace des tâches de constitution des indicateurs
Auto-évaluation	• Indisponibilité des dossiers médicaux pour l'auto-évaluation (indiquer le délai maximal d'interruption toléré -DMIA) • Non respect du secret médical lors de l'auto-évaluation • Absence de preuve de l'auto-évaluation
Tableau de bord	• Indisponibilité des indicateurs (indiquer le délai maximal d'interruption toléré -DMIA) • Erreur dans l'agrégation des indicateurs • Agrégation d'indicateurs contenant des données médicales à caractère personnel • Absence de trace des tâches de constitution des tableaux de bord

Catalogue des sinistres potentiels

Cas : Réseau de santé	**Processus : Evaluation**

Activités	**Nature du risque**
Transmission des éléments d'évaluation aux promoteurs	• Incapacité à transmettre les éléments d'évaluation aux promoteurs (indiquer le délai maximal d'interruption toléré - DMIA) • Erreur dans l'agrégation des indicateurs • Agrégation d'indicateurs contenant des données médicales à caractère personnel • Absence de trace des tâches de constitution des tableaux de bord
Actions d'amélioration des soins	• Incapacité à élaborer un programme d'actions par manque d'informations pertinentes de la part du SI du réseau de santé • Erreur dans la conception des actions d'amélioration • Publication d'un programme d'actions d'amélioration contenant des données à caractère personnel (des professionnels de santé participant, des patients du réseau)
Suivi des actions	• Impossibilité d'enregistrer les données de suivi d'actions (donner le DMIA) • Erreur dans l'enregistrement des données de suivi • Publication de données de suivi contenant des données à caractère personnel • Absence de traçabilité des données de suivi

Catalogue des sinistres potentiels

Cas : Portail ville-hôpital	**Processus : Prise de rendez-vous**

Activités	**Nature du risque**
Demande de rendez-vous	• Impossibilité de déposer une demande de RV sur l'application du portail (donner le DMIA) • Erreur dans la demande de RV • Erreur d'identification du patient • Non respect du secret médical • Absence d'accusé de réception de la demande de RV • (preuve de la demande de RV ? ? ?)
Réception demande	• Impossibilité de réceptionner la demande dans le SI de l'établissement (donner le DMIA) • Erreur dans la communication de la demande de RV • Non respect du secret médical • Absence de traçabilité des tâches automatisées • Absence de preuve en cas de litige
Détermination date de rendez-vous	• Impossibilité de fixer un RV • Erreur dans la prise de RV (patient, professionnel hospitalier) • Non respect du secret médical • Absence de traçabilité de l'activité • Absence de preuve en cas de litige (? ? ?)
Mise à disposition convocation	• Impossibilité de délivrer un RV • Erreur dans la délivrance du RV : erreur de patient, erreur de médecin destinataire,… • Non respect du secret médical • Absence de traçabilité des tâches automatisées • Absence de signalement de la mise à disposition au demandeur

Catalogue des sinistres potentiels

Cas : Portail ville-hôpital	**Processus : Prise de rendez-vous**

Activités	**Nature du risque**
Mise à disposition diagnostic et prescription	• Impossibilité de mettre à disposition les informations (donner le DMIA) • Erreur dans les informations mises à disposition • Non respect du secret médical • Absence de preuve de l'origine et de la validité des informations restituées par un professionnel de l'établissement
Mise à disposition lettre de sortie	• Impossibilité de mettre à disposition la lettre de sortie (donner le DMIA) • Erreur de destinataire de la lettre de sortie, erreur d'identification du patient • Non respect du secret médical • Pas de preuve de l'origine de la lettre ni de son authenticité

Catalogue des sinistres potentiels

Cas : Portail ville-hôpital	**Processus : Publication de l'offre de soins**

Activités	**Nature du risque**
Transformation	• Impossibilité de mettre à jour les informations (donner le DMIA) • Erreur dans la mise à jour des informations sur l'offre de soins • Non respect de la confidentialité de données personnelles • Absence de traçabilité et de validation des mises à jour • Absence de preuve de la réalisation des mises à jour (? ? ?)
Publication	• Impossibilité de publier les informations (donner le DMIA) • Publication d'informations erronées • Non respect de la confidentialité de données personnelles • Absence de preuve sur l'origine et l'authenticité des informations publiées