asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Homologation, référencement, ….

Gestion des incidents de sécurité

lundi 23 avril 2012

Agir ensemble pour soigner mieux

Ordre du jour

Gestion de de la sécurité à l'ASIP

- Le pilotage de la sécurité à l'ASIP
- La PSI
- L'organisation

Retour d'expérience sur des incidents de sécurité

- Familles de causes d'incidents
- La gestion des incidents
- Les difficultés rencontrées
- Une organisation pour la gestion des incidents
- Un formalisme commun à partager

Le pilotage de la sécurité à l'ASIP Santé

Une des missions de l'ASIP Santé est de promouvoir et encadrer le développement des systèmes d'information dans le secteur de la santé et du médico-social. A ce titre l'agence mène des activités dans lesquelles **la protection des données de santé personnelles est une priorité**.

En outre, en tant que promoteur des systèmes de partage de données de santé, autorité de certification représentant la clé de voute de l'espace de confiance santé, prescripteur de référentiels d'interopérabilité et de sécurité, **l'agence doit être exemplaire dans le management de la sécurité.**

Ce besoin de pilotage de la sécurité se traduit par la mise en place du **Système de Management de la Sécurité de l'Information** « SMSI ASIP ».

Le pilotage de la sécurité à l'ASIP Santé

Le Système de Management de la Sécurité de l'Information est la composante du dispositif de management de l'ASIP Santé qui permet de définir, mettre en œuvre, contrôler et améliorer la sécurité de l'information.

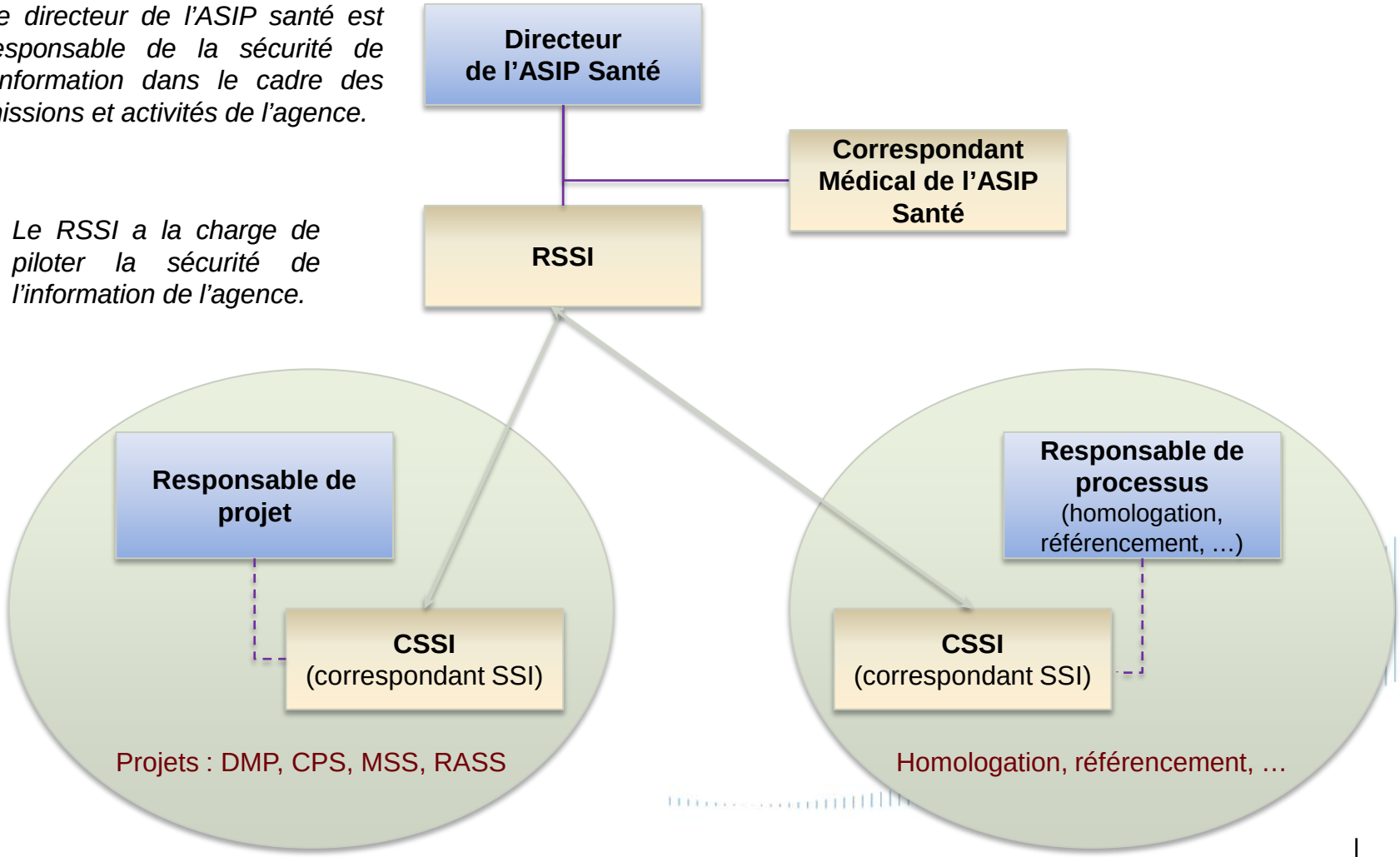
Le SMSI ASIP repose sur :

- Une politique de sécurité de l'information,
- Une organisation dédiée,
- Des processus spécifiques de gestion de la sécurité :
  - ✓ Une PSSI interne
  - ✓ Des méthodes spécifiques par projet : homologation de la DMP-compatibilité, référencement des logiciels produisant des INS, …
  - ✓ Un suivi opérationnel de la sécurité pour les projets dont nous assurons la maîtrise d'ouvrage : DMP, CPS, … (incidents, vulnérabilités)
  - ✓ Une **gestion des incidents et des vulnérabilités pour les projets internes mais aussi pour les systèmes mettant en œuvre un référencement, une homologation, … délivrée par l'ASIP Santé**

L'organisation de la SSI au sein de l'ASIP Santé

Le directeur de l'ASIP santé est responsable de la sécurité de l'information dans le cadre des missions et activités de l'agence.

Le RSSI a la charge de piloter la sécurité de l'information de l'agence.



Ordre du jour

Gestion de de la sécurité à l'ASIP

- Le pilotage de la sécurité à l'ASIP
- La PSI
- L'organisation

Retour d'expérience sur des incidents de sécurité

- Familles de causes d'incidents
- La gestion des incidents
- Les difficultés rencontrées
- Une organisation pour la gestion des incidents
- Un formalisme commun à partager

Retour d'expérience sur des incidents de sécurité potentiels

Familles de causes d'incidents observés dans les logiciels de PS/ES

- Erreur utilisateur entrainant le dépôt de document de santé dans un mauvais dossier
  - ✓ Dépôt d'un CR d'hospitalisation dans le DPI d'un autre patient et par conséquent envoi du document dans le DMP de l'autre patient.
- Confusion dans les **GAM** entre processus métier distincts (la gestion des droits au remboursement et l'attribution de l'INS) entrainant des collisions d'INS
  - ✓ INS-C de l'ouvrant droit attribué à l'ayant droit au cours de processus de gestion des droits remboursements (INS-C de la mère attribué au nouveau-né ou INS-C du mari attribué à son épouse)
- Bug logiciel dans les **GAM** entrainant des collisions d'INS
  - ✓ Attribution de l'INS-C au dernier dossier ouvert (et refermé) par l'utilisateur même si la carte Vitale n'est pas celle du patient

Retour d'expérience sur des incidents de sécurité potentiels

Familles de causes d'incidents observés dans les logiciels de PS/ES

- **Utilisation de LGC non référencés** INS-C compatibles entrainant l'attribution d'INS-C faux
  - ✓ Erreur courante des logiciels non référencés calculant l'INS-C d'ayants-droits avec le NIR de l'ouvrant droit.
- Logiciels ne respectant pas les spécifications de calcul d'INS-C entrainant l'attribution d'INS-C faux
  - ✓ Utilisation de données stockées (et modifiées) pour le calcul de l'INS-C.
  - ✓ Erreur dans les manipulation de date (cas des dates avec siècle)

Retour d'expérience sur des incidents de sécurité potentiels

Familles de causes des incidents observés dans les logiciels de PS/ES

- Erreur utilisateur entrainant le dépôt de document de santé dans un mauvais dossier
  - ✓ Dépôt d'un CR d'hospitalisation dans le DPI d'un autre patient et par conséquent envoi du document dans le DMP de l'autre patient
- Confusion dans les **GAM** entre processus métier distincts (la gestion des droits au remboursement et l'attribution de l'INS) entrainant des collisions d'INS
  - ✓ INS-C de l'ouvrant droit attribué à l'ayant droit au cours de processus de gestion des droits remboursement (INS-C de l'assuré attribué à son épouse)
- Bug logiciel dans les **GAM** entrainant des collisions d'INS
  - ✓ Attribution de l'INS-C au dernier dossier ouvert (et refermé) par l'utilisateur même si la carte Vitale n'est pas celle du patient
- **Utilisation de LGC non référencés** INS-C compatibles entrainant l'attribution d'INS-C faux
  - ✓ Erreur codage logiciel LGC non référencés calculant l'INS-C d'ayants-droits avec le NIR de l'ouvrant droit
- Logiciels ne respectant pas les spécifications de calcul d'INS-C entrainant l'attribution d'INS-C faux
  - ✓ Utilisation de données stockées (et modifiées) pour le calcul de l'INS-C.

Conséquences potentielles

Documents de santé d'un patient A dans le dossier d'un patient B (dans le DPI dans un premier temps voire propagation dans le DMP – en fonction de l'alimentation)

Conséquences

Création de doublons de dossiers

Erreur lors de l'alimentation du DMP

Ordre du jour

Gestion de de la sécurité à l'ASIP

- Le pilotage de la sécurité à l'ASIP
- La PSI
- L'organisation

Retour d'expérience sur des incidents de sécurité

- Familles de causes d'incidents
- La gestion des incidents
- Les difficultés rencontrées
- Une organisation pour la gestion des incidents
- Un formalisme commun à partager

Retour d'expérience sur les incidents de sécurité

La gestion des incidents

La procédure d'escalade suivante entre l'ASIP et les éditeurs a été mise en œuvre pour le traitement des derniers incidents :

- Détection de l'incident
  - ✓ Les incidents sont **détectés et signalés par des ES/PS ou des patients** à l'ASIP Santé.
- Identification des points de contact impliqués dans chaque organisation
  - ✓ Le point de contact est l'intermédiaire entre les organisations, en charge d'escalader l'incident au sein de son organisation qui désigne un responsable du traitement de l'incident (fréquemment le RSSI)
  - ✓ Le point de contact le plus souvent utilisé est celui renseigné pour l'homologation (DMP) ou le référencement (INS).
- Evaluation globale du périmètre, de l'impact et de la gravité de l'incident
  - ✓ Les premières actions ont pour objectif de **collecter les informations nécessaires pour évaluer de manière globale le périmètre, l'impact et la gravité de l'incident**
  - ✓ Une **coordination des actions entreprises par les éditeurs et PS/ES concernés est mise en place par le responsable de traitement désigné par l'ASIP**

Retour d'expérience sur les incidents de sécurité

La gestion des incidents

La procédure d'escalade suivante entre l'ASIP et les éditeurs a été mise en œuvre pour le traitement des derniers incidents (suite) :

- Définition du plan d'actions et traitement de l'incident
  - ✓ Le plan d'action à entreprendre pour le traitement de l'incident est proposé par l'éditeur au PS/ES et soumis à l'ASIP Santé
  - ✓ L'intervention du correspondant médical de l'ASIP Santé peut être nécessaire lorsque des analyses doivent être menées sur des données de santé.

Ordre du jour

Gestion de de la sécurité à l'ASIP

- Le pilotage de la sécurité à l'ASIP
- La PSI
- L'organisation

Retour d'expérience sur des incidents de sécurité

- Familles de causes d'incidents
- La gestion des incidents
- Les difficultés rencontrées
- Une organisation pour la gestion des incidents
- Un formalisme commun à partager

Retour d'expérience sur les incidents de sécurité

Les difficultés rencontrées

Cependant, des difficultés de mise en œuvre de cette procédure sont déjà identifiées :

- pour la détection des incidents
  - ✓ **Les incidents connus des éditeurs doivent être systématiquement remontés à l'ASIP**
- pour la mise à jour de la liste des points de contacts
  - ✓ **Les points de contact déclarés dans les procédures d'homologation à la DMP compatibilité ou de référencement INS-C sont parfois obsolètes**
- pour la coordination au niveau adéquat au sein des organisations des actions de correction (***éditeur/industriel + PS/ES + ASIP Santé***)

Il peut en résulter

- des délais de réaction face à l'incident constaté
- **des retards dans l'information des PS/ES !!**
- la persistance des incidents lorsque le déploiement des correctifs a été limité à un périmètre mal identifié (les bugs sont toujours présents dans des ES non patchés)

Ordre du jour

Gestion de de la sécurité à l'ASIP

- Le pilotage de la sécurité à l'ASIP
- La PSI
- L'organisation

Retour d'expérience sur des incidents de sécurité

- Familles de causes d'incidents
- La gestion des incidents
- Les difficultés rencontrées
- Une organisation pour la gestion des inicdents
- Un formalisme commun à partager

Retour d'expérience sur les incidents

Une organisation pour la gestion des incidents

	Patient *ES/ES* *Editeur/Industriel* *ASIP Santé*	Resp. traitement de l'incident *PS/ES*	Resp. traitement de l'incident *Editeur/industriel*	Resp. traitement de l'incident *ASIP Santé*
Détection	Incident	**Constat** Identification des Points de Contact	**Constat** Identification des Points de Contact	**Constat** Identification des Points de Contact
Evaluation		**Evaluation locale**	**Evaluation consolidée éditeur** Liste des PS/ES impactés	**Evaluation globale** Coordination Gestion du risque
Plan d'actions		**Plan d'actions local** pour le traitement de l'incident	**Définition du plan d'actions** pour le traitement dans l'ensemble des SIH/LGC concernés	**Suivi global** Coordination

Ordre du jour

Gestion de de la sécurité à l'ASIP

- Le pilotage de la sécurité à l'ASIP
- La PSI
- L'organisation

Retour d'expérience sur des incidents de sécurité

- Familles de causes d'incidents
- La gestion des incidents
- Les difficultés rencontrées
- Une organisation pour la gestion des incidents
- Un formalisme commun à partager

Retour d'expérience sur les incidents

Un formalisme commun à partager

Au sein de l'ASIP, le traitement de chaque incident est formalisé dans une fiche qui contient

- la synthèse de l'état du traitement de l'incident
  - ✓ Le modèle de fiche d'incident contient une synthèse mise à jour au fur et à mesure du traitement de l'incident.
- la consignation des actions entreprises et des résultats obtenus
  - ✓ La fiche d'incident contient l'historique (minutes) de toutes les actions entreprises de la détection à la résolution de l'incident ainsi que les résultats obtenus
- les informations nécessaires au retour d'expérience a posteriori
  - ✓ Les fiches d'incidents sont exploitées par l'ASIP Santé pour améliorer le processus de gestion des incidents

Ce modèle de fiche d'incident peut être mis à disposition des éditeurs pour partager un formalisme commun pour la gestion des incidents

La DMP compatibilité,
le référencement INS-C,
…,
la fin d'un travail, le début d'une obligation

Jean-François PARGUET
Directeur du Pôle Technique et Sécurité
T. 01 58 45 33 59 - M. 06 31 76 39 29

asipsanté
Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
esante.gouv.fr