GROUPEMENT HOSPITALIER NAMUROIS

La sécurité informatique

Philippe Santantonio

Le développement de la gestion des risques à l'hôpital, impact et perspectives

Congrès CIPIQ-S
Luxembourg, 4 octobre 2011

Agenda

- Introduction
- Les types de menaces
- Une problématique concrète
- Evaluer sa sécurité informatique
- Etude de cas : aspects humains
- Conclusions
- Questions/réponses

Tenir compte du risque informatique?

L'informatique déborde du cadre administratif et touche de + en + d'acteurs

- En interne : chaque secteur a son applicatif. Les divers applicatifs « communiquent »
- En externe vers d'autres systèmes d'informations : réseau de santé, médecins traitants, …
- En externe vers le patient

Typologie des risques

Les menaces qui peuvent affecter un système informatique sont très variées mais peuvent être classées selon 3 axes

- Les accidents
- Les erreurs
- Les malveillances

Typologie des risques : les accidents

- Destruction partielle ou totale : incendie, inondations, climatisation
- Panne du matériel ou du logiciel

- Précautions à prendre
  - Mot clé : « redondance »
  - Backup (régulier, fréquent, automatique, hors-site, tests réguliers)
  - Contrat de maintenance avec engagement SLA du fournisseur
  - Disponibilité du personnel technique

Typologie des risques : les erreurs

- Erreurs de saisie
- Erreurs lors du transfert de l'information
- Erreurs de conception

- Précautions à prendre
  - Tests à priori
  - Tests à postériori : contrôles croisés
  - Sensibilisation du personnel

Typologie des risques : les malveillances

- Vol ou destruction de matériel
- Détournement ou altération des données

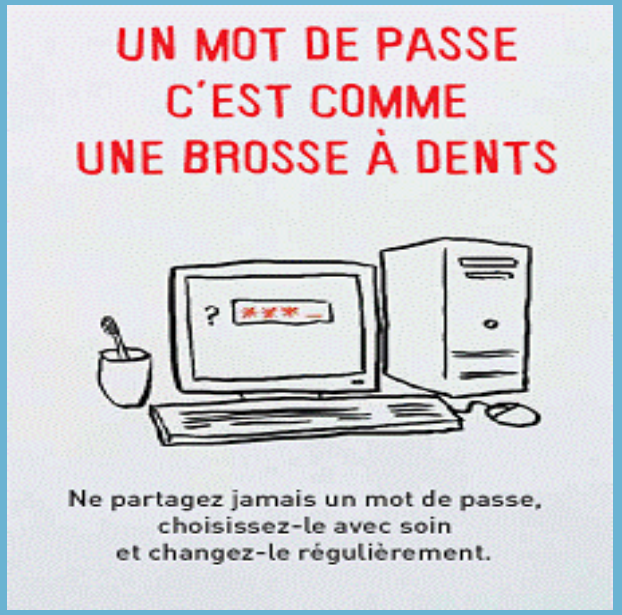
- Précautions à prendre
  - Sécurisation physique
  - Gestion et contrôle des accès, traçabilité, audit
  - Outils de supervision du réseau : virus, intrusions, logiciels espions, …
  - Les backup

Problématique du mot de passe (mdp)

www.casafree.com

Faiblesses du mot de passe

- Trop court
- Trop simple
- Il est personnel
- Il est parfois noté sur un post-it placé sous le clavier
- Il n'est pas changé assez fréquemment
- Le même mdp est utilisé pour divers accès



www.cases.public.lu/fr

Comment se souvenir du mdp ?

- Phrase magique : vous composez une phrase (que vous mémorisez), les premiers caractères de chaque mot (ainsi que les signes de ponctuation) forment votre mot de passe
  Ex : « Jupilor ? Les hommes savent pourquoi ! » génère le mdp suivant « J?Lhsp! »

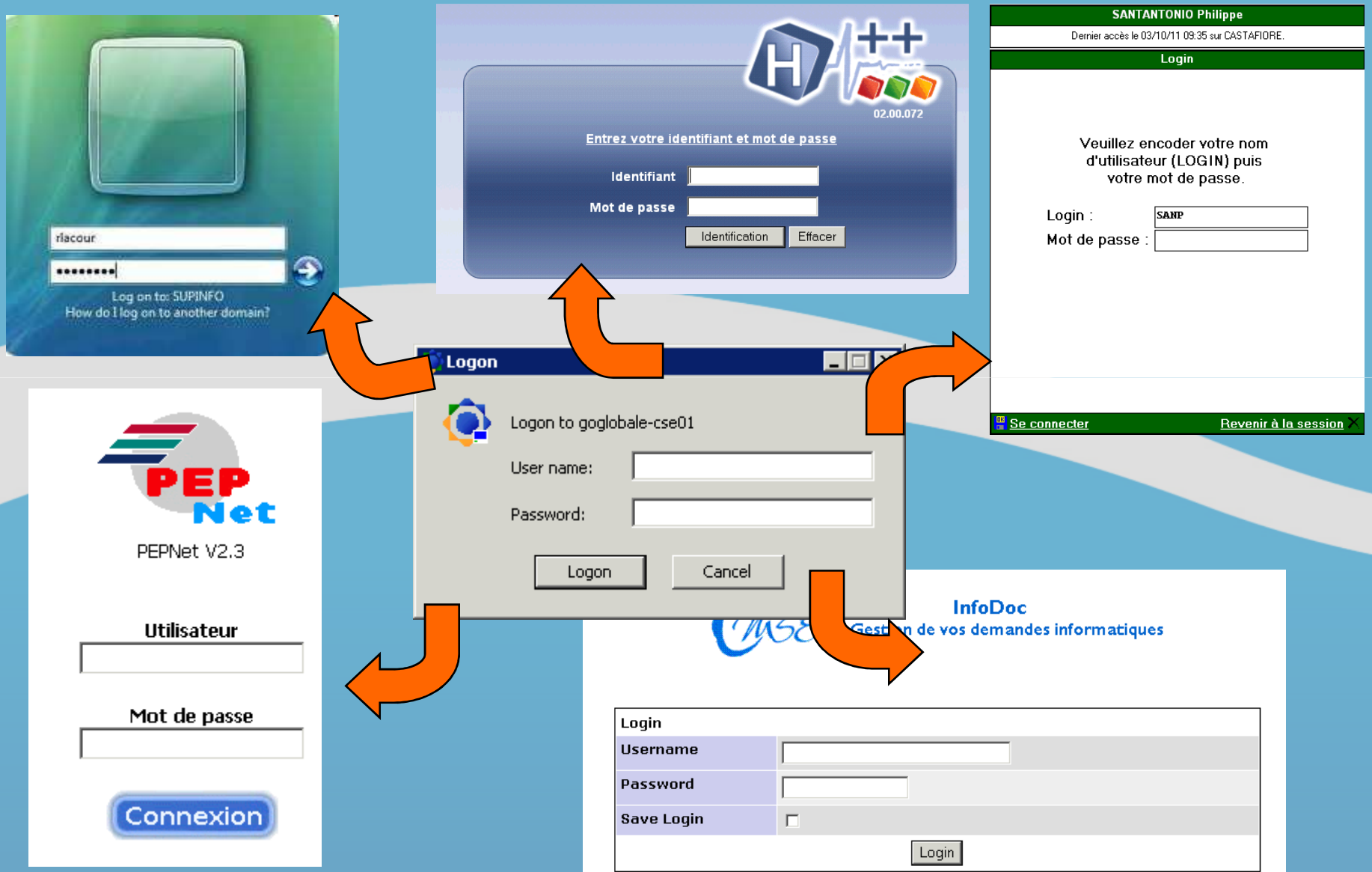
- Technique phonétique : utiliser les sons de chaque syllabe pour fabriquer un mot facile à retenir.
  Ex : « J'ai acheté 8 CD pour 100 euros cet après-midi » devient « ght8CD%E7am »

- Utiliser un logiciel (ex www.keepass.info)

Une solution technique ? Le SSO.

- SSO : Single Sign On = Authentification unique
- Principe : L'utilisateur ne s'authentifie qu'une seule fois pour accéder à plusieurs applications

Le SSO, comment cela fonctionne ?



SSO : les avantages

- Pas d'obligation de se souvenir de plusieurs mdp
- Réduction du temps passé pour l'introduction du mdp
- Réduction du nb d'appels au helpdesk pour les mdp oubliés
- Automatisation des changements de mdp
- Respect des règles de sécurité en termes de choix de mdp

SSO : quelques gains collatéraux

- Centralisation des droits d'accès
- Politique de contrôle des accès en fonction des points d'accès et des horaires
- Traçabilité des connexions des utilisateurs
- Mode kiosque : changement rapide d'utilisateur
- Délégation des droits des utilisateurs (attention à l'aspect signature)

SSO : les critiques

- Les données d'accès des utilisateurs sont centralisées dans un référentiel qui doit être particulièrement sécurisé

- Une personne mal intentionnée qui connaîtrait le mdp global de l'utilisateur pourrait avoir accès à toutes ses ressources

- Solution : combiner plusieurs méthodes d'identification
  - Ce que l'on sait : un mot de passe
  - Ce que l'on détient : clé USB, badge, carte eID
  - Ce que l'on est : iris, empreinte digitale

Comment évaluer le niveau de sécurité informatique de mon institution ?

- ISO 27001 : norme relative à la sécurité de l'information au sens large
- ISO 27002 : code de bonnes conduites pour la sécurisation de l'information. Propose des centaines de contrôles de sécurité/mécanismes de sécurité potentiels
- ISO 27799 : transpose ISO 27002 au domaine de la santé

Outil d'auto-évaluation du GMSIH

GMSIH : groupement pour la modernisation du système d'information hospitalier (www.gmsih.fr)

Association française créée en 2000

A produit un guide d'auto-évaluation

- Évaluer le niveau de maturité en termes de sécurité
- Identifier le niveau de risque
- Déterminer les actions prioritaires

Outil très simple, feuille de calcul Excel

Questionnaire de 100 questions

Questionnaire d'auto-évaluation

100 Questions AESSI v 1.00

Questions	Questions	Choix	Contrôle
N° Principes	**Chap.2.3 : Sécurité physique et Sécurité de l'environnement**		
2.3 1 - 1	« L'établissement a-t-il établi un périmètre de sécurité dans l'établissement et déterminé clairement des zones de sécurité en fonction de la sensibilité des informations et des infrastructures ? »	Définition du périmètre de sécurité global de l'établissement.	OK
2.3 2 - 2	« L'établissement a-t-il mis en place un contrôle d'accès physique comprenant plusieurs niveaux d'habilitation selon la sensibilité des zones accédées ? »	Mise en place d'un contrôle d'accès uniquement aux zones très sensibles.	OK
2.3 2 - 3	« Les configurations et les postes informatiques et réseaux sensibles sont-ils secourus en cas de rupture de l'alimentation électrique normale ? »	Un secours électrique a été prévu pour les installations informatiques et réseaux sensibles.	OK
2.3 2 - 4	« Les chemins de câbles, armoires de brassage et baies, sont-ils protégés contre les accidents physiques, les erreurs et les malveillances internes et externes ?»	Chemins de câble, baies et armoires protégées contre les accidents physiques et les erreur	OK

Questionnaire de 100 questions

Questionnaire d'auto-évaluation

10 Quest
AESSI

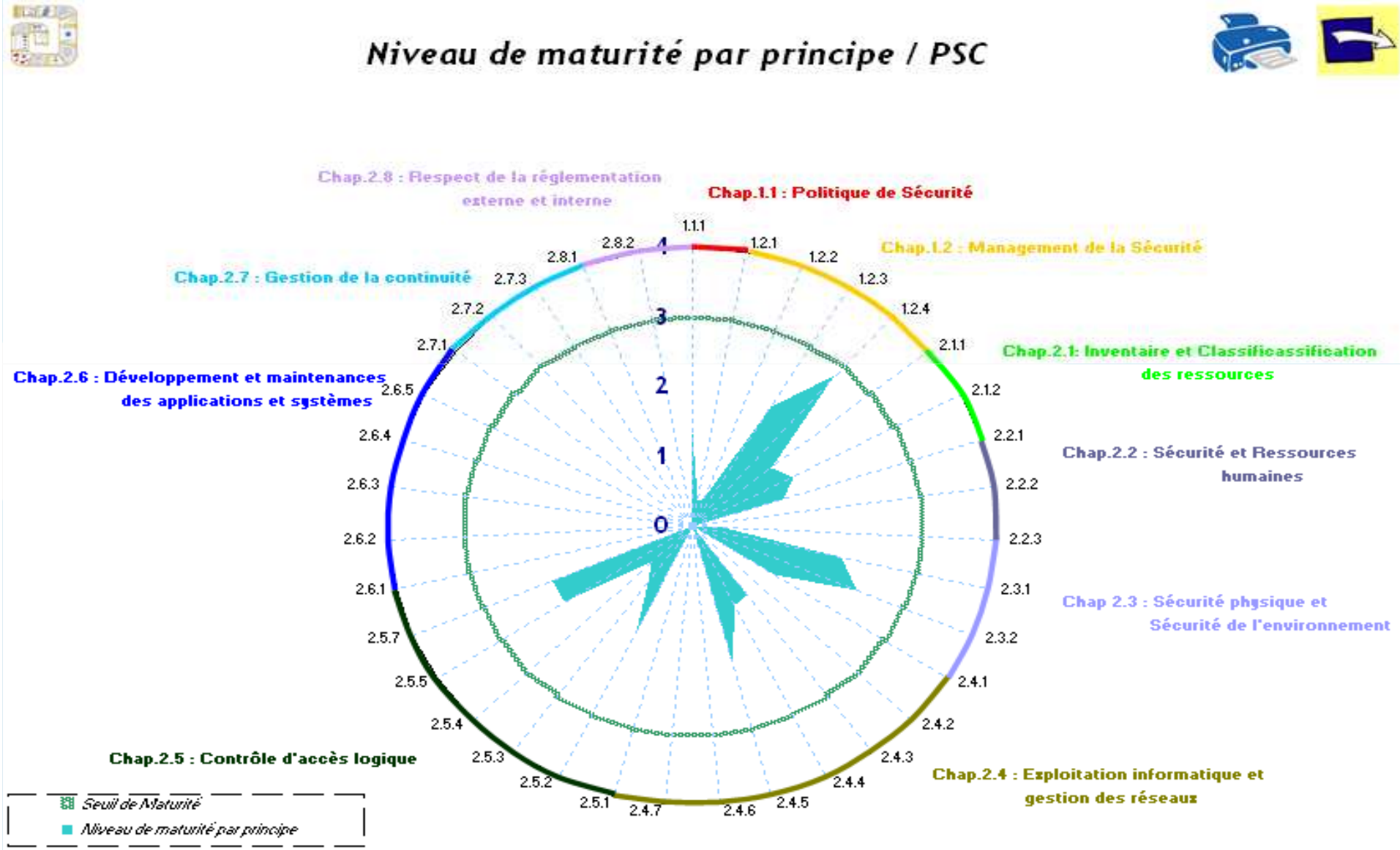
Questions	Questions	Choix
N° Principes	**Chap.2.3 : Sécurité physique et Sécurité de l'environnement**	
2.3 1 - 1	« L'établissement a-t-il établi un périmètre de sécurité dans l'établissement et déterminé clairement des zones de sécurité en fonction de la sensibilité des informations et des infrastructures ? »	Définition du périmètre de sécurité global de l'établissement.
2.3 2 - 2	« L'établissement a-t-il mis en place un contrôle d'accès physique comprenant plusieurs niveaux d'habilitation selon la sensibilité des zones accédées ? »	Mise en place d'un contrôle d'accès uniquement aux zones très sensibles.
2.3 2 - 3	« Les configurations et les postes informatiques et réseaux sensibles sont-ils secourus en cas de rupture de l'alimentation électrique normale ? »	Un secours électrique a été prévu pour les installations informatiques et réseaux sensibles.
2.3 2 - 4	« Les chemins de câbles, armoires de brassage et baies, sont-ils protégés contre les accidents physiques, les erreurs et les malveillances internes et externes ?»	

Résultats sous forme numérique

Niveau de maturité atteint par principe

N° des Chapitres et Libellés	N° des Principes	Libellé des principes	Niveau (de 0 à 4)
1.1 Politique de Sécurité			
	1.1.1	Politique de Sécurité de l'information	1,33
1.2 Management de la Sécurité			
	1.2.1	Organisation de la Sécurité	0,36
	1.2.2	Stratégie de mise en œuvre	0,40
	1.2.3	Sensibilisation	2,00
	1.2.4	Sécurité des interventions par des tiers externes	2,86
2.1 Inventaire et Classification des ressources			
	2.1.1	Inventaire des ressources	1,33
	2.1.2	Classification des ressources	1,50
2.2 Sécurité et Ressources humaines			
	2.2.1	Sécurité dans la définition des postes et des ressources	1,25
	2.2.2	Formation du personnel à la sécurité de l'information	0,00
	2.2.3	Réactions aux incidents de sécurité et aux défauts de fonctionnement	0,40
2.3 Sécurité physique et Sécurité de l'environnement			
	2.3.1	Etablissement et protection d'un périmètre de sécurité	2,00
	2.3.2	Protection et sécurité du matériel	2,33
2.4 Exploitation informatique et gestion des réseaux			
	2.4.1	Procédures d'exploitation et responsabilités	1,27
	2.4.2	"Planification de la Capacité" et recette pour mise en exploitation	0,00
	2.4.3	Protection contre les logiciels pernicieux	1,22
	2.4.4	Sauvegarde et journaux d'exploitation	1,25
	2.4.5	Gestion des réseaux	2,00

Résultats sous forme graphique

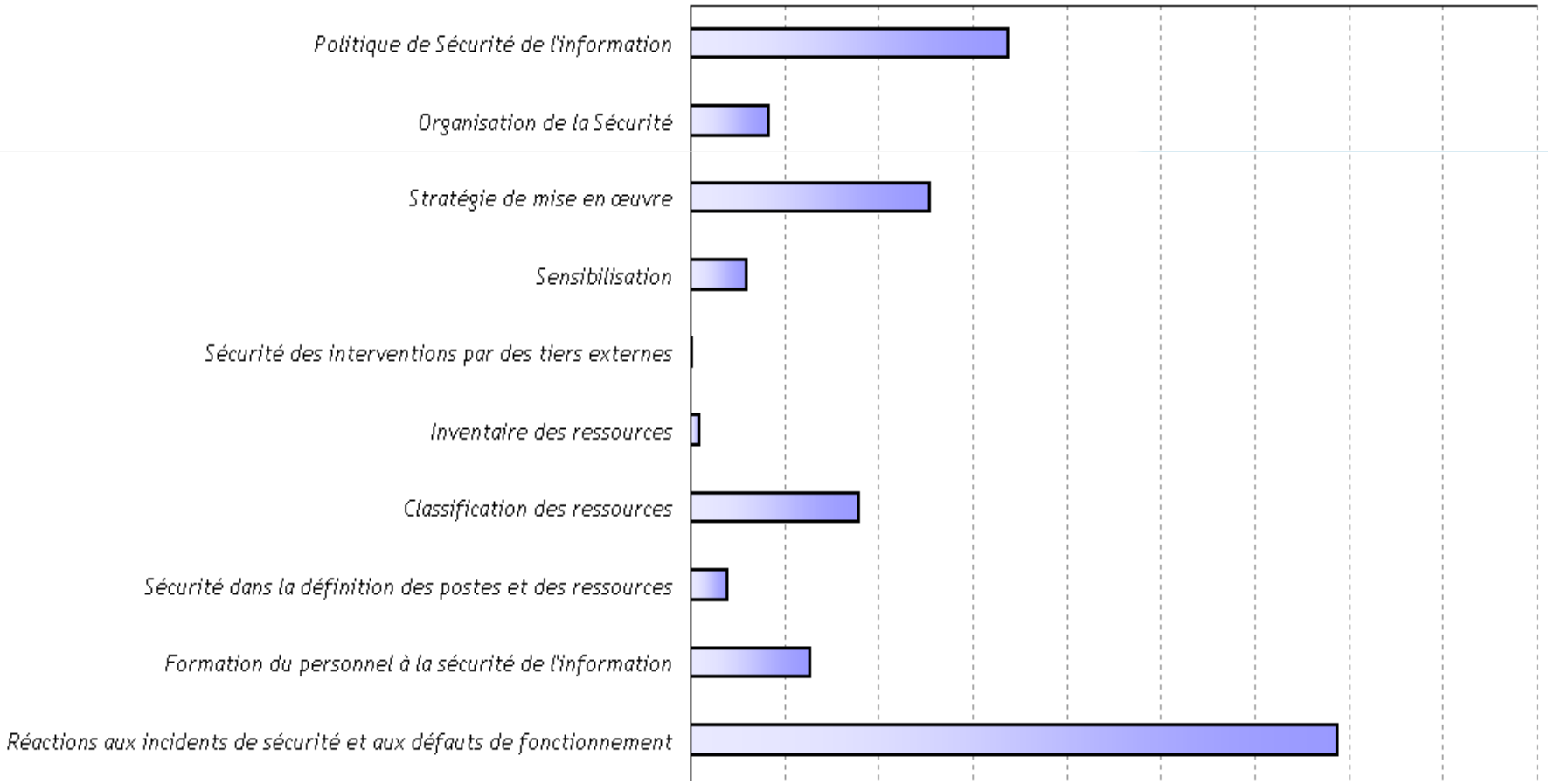


Gravité des risques

Efficacité des principes

Image 5

Efficacité des principes en réduction des risques

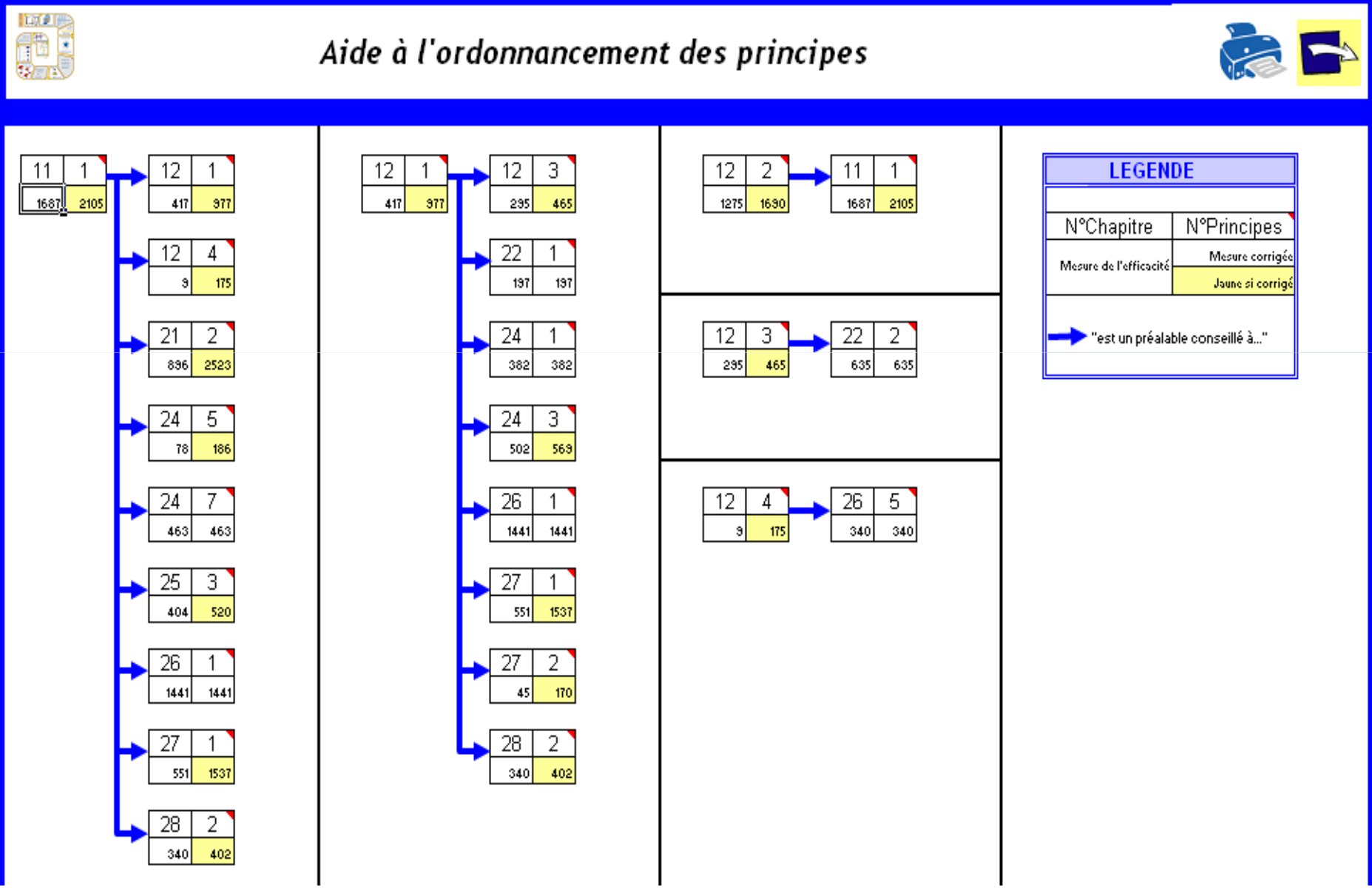


Principes triés par efficacité

Principes triés selon leur efficacité en terme de réduction de risquepour l'E.S

Ordre	*Principe*	*Libellé*	*Efficacité*
1	2.5.1	Expression des exigences de l'établissement en matière de contrôle d'accès logique	4150
2	2.2.3	Réactions aux incidents de sécurité et aux défauts de fonctionnement	3436
3	1.1.1	Politique de Sécurité de l'information	1687
4	2.6.1	Intégration de la sécurité dans les développements	1441
5	1.2.2	Stratégie de mise en œuvre	1275
6	2.4.6	Manipulation et sécurité des supports	1182
7	2.6.3	Cadre de mise en œuvre des mécanismes cryptographiques de sécurité	926
8	2.1.2	Classification des ressources	896
9	2.2.2	Formation du personnel à la sécurité de l'information	635
10	2.7.1	Prise en compte des exigences de disponibilité de l'établissement	551
11	2.4.3	Protection contre les logiciels pernicieux	502
12	2.4.7	Echanges d'informations et de logiciels	463
13	1.2.1	Organisation de la Sécurité	417

Ordonnancement des principes



La sécurité informatique, une assurance « tous risques » ?

Incident « fraxiparine »

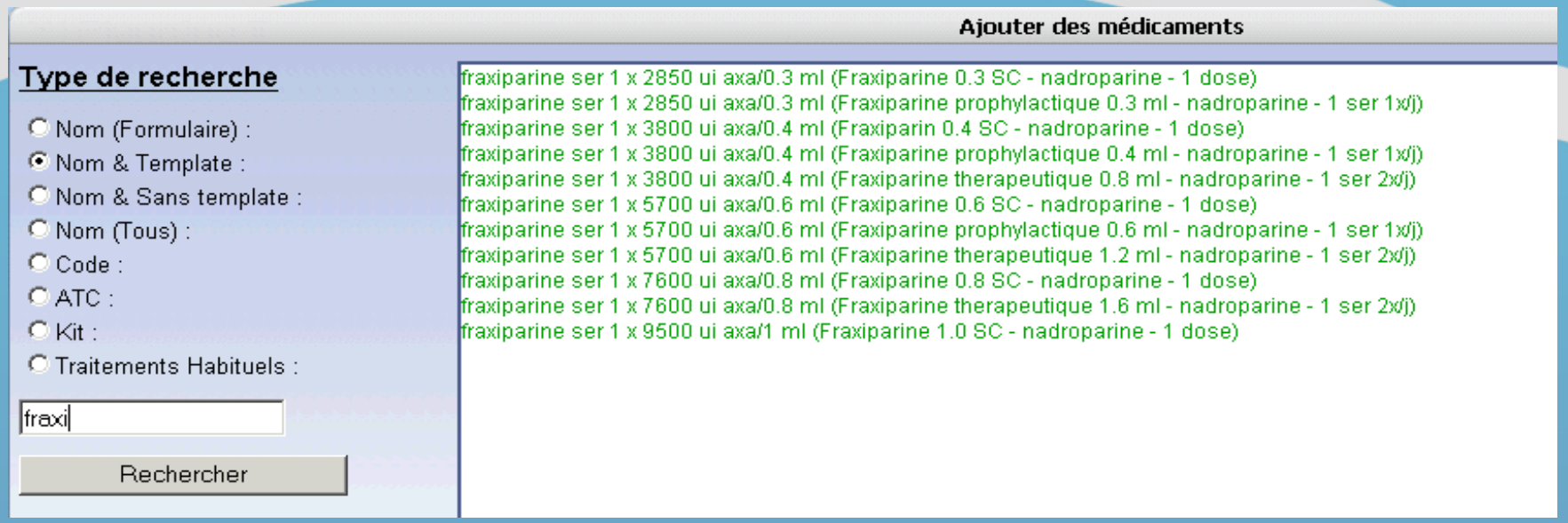
Mr. L hospitalisé pour un problème de pace maker a reçu de la fraxiparine tous les jours à 20h à partir du lendemain de son électrophysiologie au lieu de recevoir une dose de fraxiparine le jour de l'électrophysiologie à 21h. Ce patient, devant être opéré pour placement de pace maker quelques jours plus tard, a saigné et a développé un hématome.

Incident « fraxiparine »

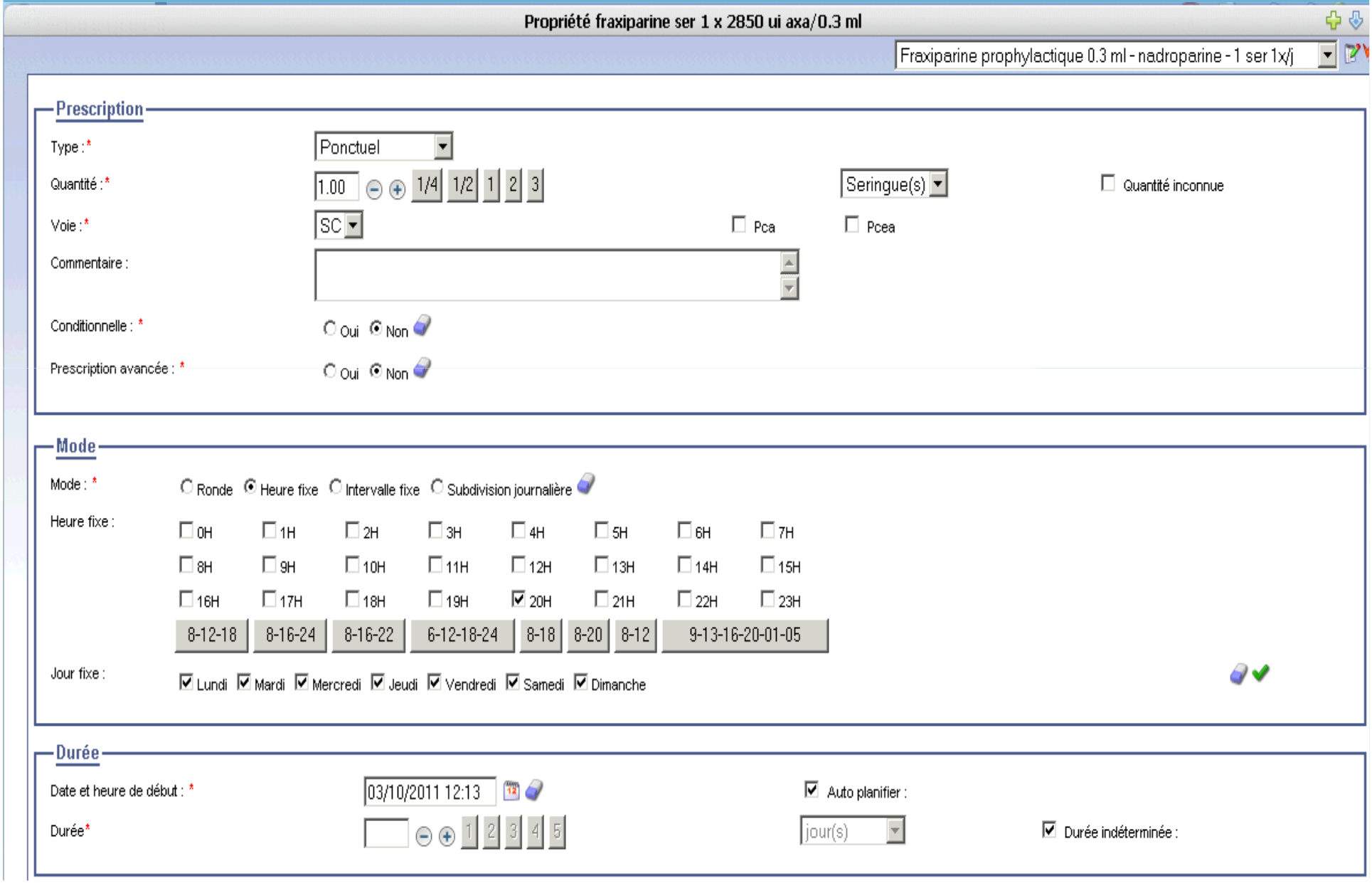
En salle technique, le médecin prescrit 1 dose de fraxiparine à 21h pour 1 jour

Dysfonctionnement 1

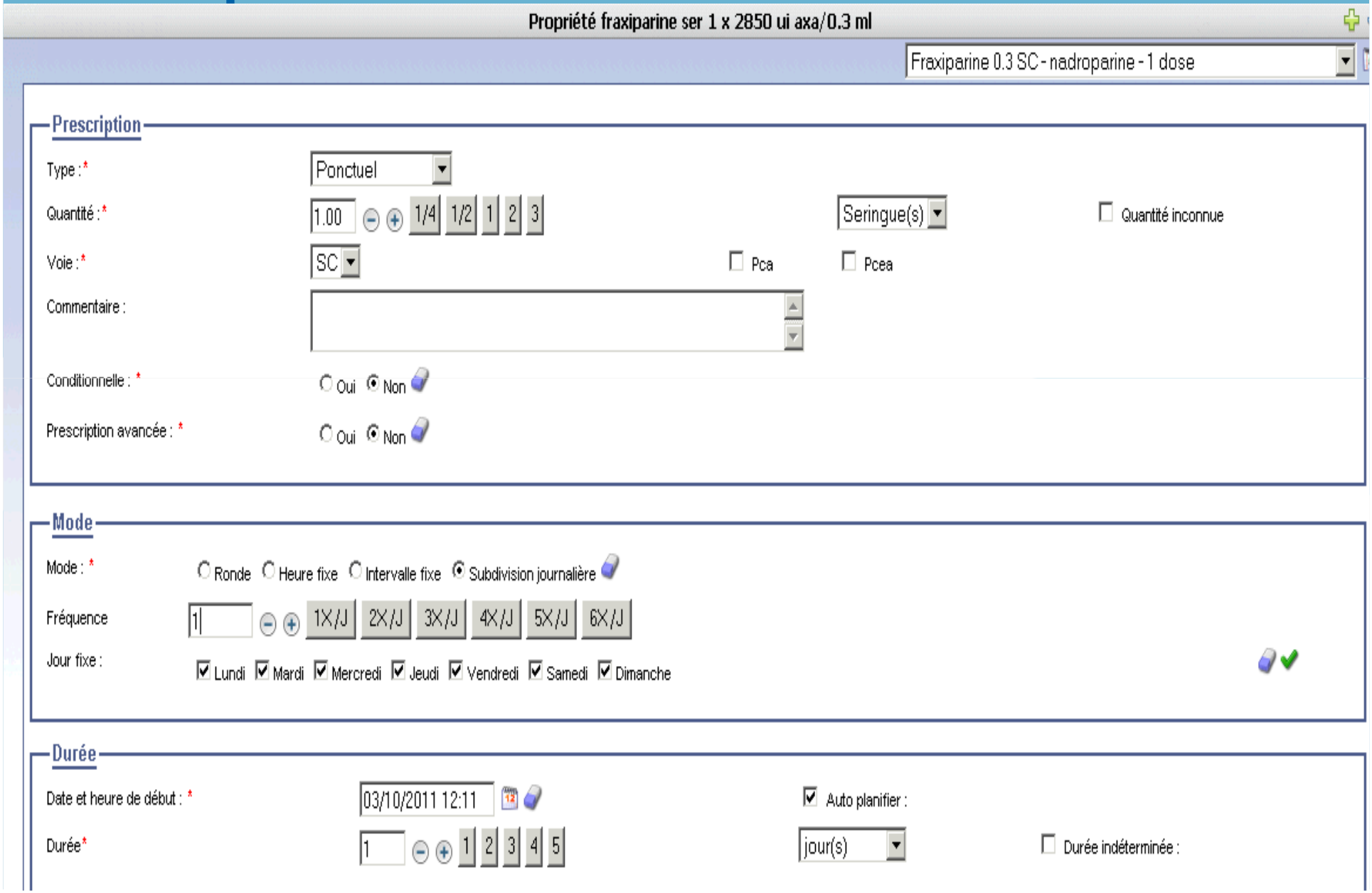
- L'infirmière choisit *fraxiparine 1ser 1x/j* au lieu de *fraxiparine 1 dose*



Fraxiparine 1x/jour



Fraxiparine 1 dose



Incident « fraxiparine »

Dysfonctionnement 2 :

Le médecin valide le traitement encodé par l'infirmière dans un écran où il ne voit pas les détails de la prescription. Il ne remarque donc pas l'erreur d'encodage.

Incident « fraxiparine »

Dysfonctionnement 3 :

La révision journalière des traitements par le médecin d'étage et l'infirmière aurait dû les alerter sachant que ce patient devait être opéré quelques jours plus tard

Incident « fraxiparine »

Dysfonctionnement 4 :

Le personnel soignant a bénéficié d'une formation relative au logiciel de prescription. Le concept de planification semble complexe et a peut-être été sous-estimé.

Conclusions

- Ambivalence de l'outil informatique en termes de gestion des risques:

D'une part : merveilleux outil centralisateur des données qui assure une traçabilité et qui facilite les activités des prestataires de soins

D'autre part : il génère une dépendance de ces acteurs vis-à-vis d'un système d'informations de plus en plus complexe et ouvert vers l'extérieur

Conclusions

- l'informatique ne supprime pas les risques, il en génère d'autres. Le respect des règles de sécurité informatique doit permettre d'en limiter les conséquences.
- Même si l'informatique est un domaine profondément technique, n'oublions les aspects humains.

GROUPEMENT HOSPITALIER NAMUROIS

Des questions ?

GROUPEMENT HOSPITALIER NAMUROIS

Clinique Saint-Luc
Rue Saint-Luc 8, B-5004 Bouge
+32 (0)81 20 91 11
info@slbo.be
www.saint-luc-bouge.be

Clinique et Maternité Sainte-Elisabeth
Place Louise Godin 15, B-5000 Namur
+32 (0)81 72 04 11
info@cmsenamur.be
www.cmsenamur.be

Foyer Saint-François
Rue Louis Loiseau 39a, B-5000 Namur
+32 (0)81 74 13 00
secretariat@foyersaintfrancois.be
www.foyersaintfrancois.be