



Sécurité du Système d'Information

Cyril PATRIGEON – CISME - Mai 2014

Contexte

- ▶ Un contexte réglementaire important:
 - ▶ Loi Informatique et Liberté (1978)
 - ▶ Arrêté du 5 Mars 2004 sur les bonnes pratiques
 - ▶ Décret 2007-960 relatif à la confidentialité des informations médicales
 - ▶ Article L-1111-8 du code de la santé publique sur l'hébergement
 - ▶ Rapport 2004 sur le DMST
 - ▶ La PGSSI préconisée par l'ASIP-Santé
 - ▶ Le code Pénal, le code de la Santé publique et la Déontologie Médicale

- ▶ Actuellement très peu d'organismes sont en adéquation avec les lois

Une sécurité organisée

- ▶ Une politique de sécurité appuyée par la Direction
- ▶ Un engagement de la Direction (organisation, attribution)
- ▶ Schéma directeur SSI diffusé
- ▶ Gestion des actifs (identification, classification, responsabilité)
- ▶ Intégration des RH à la SSI (fiche de poste, charte, procédures, sensibilisation)

La sécurité physique et métier

- ▶ Une exploitation en accord avec le besoin
 - ▶ Des bonnes réponses aux exigences métiers
 - ▶ Prendre en compte les aspects réglementaires
 - ▶ Un PCA / PRA robuste, testé et qui tient compte de la SSI
- ▶ Une sécurité physique proportionnée
 - ▶ Des zones publiques
 - ▶ Des zones d'accès surveillé
 - ▶ Des zones d'accès réglementé et protégé

La sécurité logique

- ▶ Authentification forte des utilisateurs, et des objets
- ▶ Séparation physique des données médicales et des autres données
- ▶ Sécurisation* permanente des données médicales sur tous les supports, chiffrement des transmissions hors site
 - *: la CNIL préconise un chiffrement permanent*
- ▶ Une journalisation permanente et séparée.
- ▶ Une architecture globale réfléchie avec la sécurité

Que faire ?

- ▶ Etat des lieux
- ▶ Schéma directeur
- ▶ Organiser la SSI et mener les actions prioritaires (en fonction des risques identifiés)
- ▶ Penser la SSI de manière itérative



Merci de votre attention.

Des questions ?

7

Cyril PATRIGEON

Expert Sécurité des SI santé



- IT Risk Management Expert
- Expert, Administrator and Treasurer at Club EB IOS
- Email: cyril@patrigeon.net
- Linked In: <http://www.linkedin.com/in/cyrilpatrigeon>
- Twitter: @CyrilPatrigeon
- Blog SSI: <http://cyril.patrigeon.net>
- Gsm: 06.45.99.55.41