Sécurité de l'Information Hospitalière - ISO 27799

Permettre aux hôpitaux de connaître leur niveau de sécurité de l'Information - Exigence de la HAS

CONTEXTE

Définitions :

• Disponibilité : Propriété d'être accessible et utilisable à la demande par une entité autorisée

• Confidentialité : Propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, […] non autorisées

• Intégrité : Propriété de protection de l'exactitude et de l'exhaustivité des actifs

Réglementation du secteur hospitalier :

• Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : Art29

• Charte sur le respect de la confidentialité

• Loi Kouchner du 4 mars 2002

• Exigences de la Haute Autorité à la Santé

Enjeux :

• Respecter les exigences de la HAS afin d'être certifié sur le référentiel HAS

• Renforcer la confiance du patient en l'hôpital

QUELQUES CHIFFRES…

Critères	Résultats
Nombre d'hôpitaux certifiés ISO 27799 en France	Aucun
Responsable sécurité identifié	35% des hôpitaux en 2008 ET 43% en 2010
Hôpitaux ayant procédé à l'inventaire leurs informations	57% en 2009 dont 48% ont classé leurs informations selon les critères de disponibilité, confidentialité et intégrité

INTERÊT DE L'OUTIL

• **Pour qui ?**

Personne qui gère le système de sécurité de l'information en centre hospitalier

• **Pourquoi ?**

Pour évaluer son système de sécurité dans le but de réaliser des actions préventives et / ou correctives

UTILISATION DE L'OUTIL D'AUTODIAGNOSTIC

1. Remplir la grille à l'aide des menus déroulants, ainsi que les cases oranges et jaune pâle si nécessaire
2. Visualiser les résultats sous forme de tableaux
3. Visualiser les résultats sous forme de graphique

A.II.3	Communication	
C30	Les utilisateurs sont informés de la confidentialité des dossiers	VRAI
C31	Les copies des dossiers sont étiquetées confidentielles	FAUX / PLUTÔT FAUX / PLUTÔT VRAI / VRAI
C32	Des avertissements sont placés dans les ascenseurs, sur les portes derrière lesquelles les échanges oraux ont lieux ainsi que dans d'autres zones	

Titre	Résultat (%)
Gestion de la documentation	79
Gestion des risques	100
Amélioration continue	100

AMELIORATIONS ET PERSPECTIVES

- Veiller à l'évolution du référentiel de la HAS
- Une exigence de la HAS à satisfaire : « le dispositif de sécurité du système d'information est évalué et fait l'objet d'actions d'amélioration »
- Mettre la grille d'autoévaluation sous forme de formulaire
- Faire tester l'outil par plusieurs hôpitaux
- Faire évoluer la grille en fonction de l'évolution des exigences

BIBLIOGRAPHIE

• Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : http://www.legifrance.gouv.fr

• Exigences de la Haute Autorité à la Santé : http://www.has-sante.fr

• Menaces informatiques et pratiques de sécurité en France publié par le CLUSIF : http://www.clusif.asso.fr

• NF EN ISO27799 Septembre 2008 (Gestion de la sécurité de l'information relative à la santé) : http://sagaweb.afnor.org