

Executive Certificate : Les nouveaux défis du système d'information en matière de Santé et de E-Santé

La gestion de la qualité, sécurité et continuité d'activité

Nous sommes à un moment singulier. L'informatique pénètre « partout ». Nous modifions notre système de santé avec l'introduction de bouleversement en termes de management. Des projets de réseaux ou de pôles de Santé se multiplient dans toutes les régions. Ils ont pour objectif principal de faciliter la communication et la coordination entre des professionnels de santé, ou du domaine social, exerçant sur un territoire. Des projets de Dossier Patient et Gestion de la connaissance accompagnent ces organisations et établissements de santé.

Les technologies utilisées dans ces réseaux représentent de réels risques et des fragilités :

- Existence de dispositifs de piratage en libre service sur Internet
- Atteinte du patrimoine informationnel (procédure, recherche..) de l'établissement
- Virus transmis en pièce jointe dans les messageries personnelles et professionnelles
- Saturation des systèmes par l'envoi de messages répétés
- Usurpation d'identité facilitée ... Le réseau manipulant des flux financiers (paiement d'actes, feuille de soins électronique,...)

Les professionnels de santé (directeurs, médecins, pharmaciens...) doivent acquérir de nouveaux comportements. Si, ils ont pour leurs activités, classiquement une obligation de moyen, ils sont soumis pour leurs systèmes informatique à une obligation de résultat et de continuité de service. La qualité et la sécurité de l'informatique participe à la qualité et la sécurité des soins et de la prise en charge.

OBJECTIFS

- Bâtir une analyse de risque, globale liée à l'usage des systèmes d'information, de l'informatique et télécoms.
- Conduire un audit de sécurité informatique et télécoms ISO 2700X sur un périmètre santé.
- Choisir et intégrer dans un système d'information un progiciel applicatif sur et de qualité, Intégrer une nouvelle technologie (rfid, robot,..) ou une nouvelle pratique ou chemin clinique (téléconsultation clinique, ..) dans le système existant.
- Identifier et contrôler les accès du personnel de santé, des patients et des biens : maîtrise des 3 critères d'identification, traçabilité humaine et contrôle d'accès au système d'information, identitovigilance.
- Etablir la continuité de service et d'activité dans l'offre de soins et Plan de continuité en cas de sinistre, de malveillance et de pandémie, maintenance en condition opérationnelle (MCO) et gestion de crise.
- Connaître la sécurité du réseau informatique interne et externe.
- Connaître les coûts de la sécurité, réduire les coûts cachés et de la non qualité.
- Identifier, valoriser et protéger le patrimoine informationnel (EPP, procédure de santé, recherche clinique, e learning..)
- Connaître les aspects juridiques de l'usage de l'informatique en matière de soins médicaux (la preuve par e-mail et archivage des e mails,..).

PARTICIPANTS CONCERNÉS

- Directeurs d'établissement, direction SI, Responsable Sécurité SI, Gestionnaire des risques, Médecins, Présidents de CME, DIM,
- Cadres de l'Agence Régionale de Santé, de l'Assurance Maladie
- Industriel de l'informatique et de l'électronique de Santé, et SSII
- Toute personne intéressée par le management hospitalier et la qualité-sécurité des systèmes d'information en Santé.

Méthodes pédagogiques

- Etudes de cas
- Cas pratiques
- Conférences
- Mise en application immédiate des méthodes
- Travail de groupe organisé entre les séances pour être présenté en validation

Responsables pédagogiques

- M. Vincent LEROUX
Médecin de Santé Publique
Professeur à l'ECP
Co-Responsable du Mastère Spécialisé « Gestion des risques et de la sécurité des établissements et réseaux de Santé ».
- M. Paul de KERVASDOUE
Expert en Sécurité informatique
Enseignant à l'ECP

Dates

- Du 16 au 18 novembre 2011
- Du 14 au 16 décembre 2011
 - Du 5 au 6 janvier 2012
 - Du 16 au 18 janvier 2012
 - Du 15 au 17 février 2012
 - Du 15 au 16 mars 2012

Lieu

- (16 jours : 112 heures)
- Châtenay-Malabry (92)

Conditions de participation

- Réf. ST14 : 6 500 € HT (Restauration offerte)
- Joindre un CV et une lettre de motivation

Information & inscription

- Christelle GROUAS
- Tél. : + 33 (0)1 41 13 14 02
- E-mail : sante@cf.ecp.fr

Développer un programme "sur-mesure", nous consulter

PROGRAMME

Module n°1 : Cible, périmètre objectifs et concepts de base de la qualité et de la sécurité des systèmes d'information de santé.

- Concepts, Cible et périmètre de la sécurité informatique et télécoms en santé Périmètre des systèmes d'information et des STIC en Santé
- Organisation de la sécurité et de la qualité de la eSanté (HS2, ..) en France (ASIP, ANAP, CNIL, Ordres, Afnor...)
- Risques et sécurité informatique des industries de santé (Laboratoires pharmaceutiques, éditeurs de logiciels ..)
- Gouvernance des risques en matière de santé (place du RSSI/DSIO)

Module n°2: Droit et assurance en matière de qualité et de sécurité du système d'information de santé

- Le droit en matière de sécurité dans le domaine de la santé : Droit des patients, CNIL, Charte de Cyber surveillance, droits d'auteurs Responsabilité civile contractuelle et limites avec la Responsabilité délictuelle en Santé
- L'assurance Perte d'Exploitation Informatique pour financer la reprise informatique après une panne ou un sinistre.
- Sécurité informatique et aspects juridiques, contractuels de la sous-traitance

Module n°3 : Méthodes d'analyse de risque, de diagnostic, de sécurité informatique et télécoms

- Plan d'orientation Sécurité ou Schéma Directeur ISO 2700X Audit ISO 27001 – Identification (IAM) et Contrôle d'accès physiques et logiques, identitévigilance
- Analyse de risque et évaluation de la sécurité des produits sensibles : cartes CPS, clés USB Firewall etc. Common Critéria ISO 15408 – Approche technico-commerciale
- Analyse de risque des TIC des industriels des produits de santé
- Sécurité des applications informatiques – et sous traitance Cloud Computing
- La sécurité d'un réseau Intranet, Extranet Internet en santé
- Bâtir un plan de continuité d'activité (PCA) en informatique de soins – Théorie et norme BS 25999 ; Archivage traçabilité des données numériques (dossiers médicaux et patients au sens large)

Module n°4 : Les Produits, les réseaux et les services

- Sécurité des réseaux numériques appliquée aux réseaux, établissements de santé
- La sécurité des cartes santé : Contrôle d'accès, badges, Vitale et CPS
- La sécurité des produits télécoms Sécurité d'un réseau de soins ouvert
- Qualité et sécurité des contenus (dossiers patients, moteur de recherche, internet, HoNcode, netscoring)
- Management opérationnel du DSI/RSSI, Attaques Internet, gestion des personnels et ressources externes

Module n°5 : Mécanismes – Mise en œuvre des méthodes – Cas pratiques – Retour d'Expérience

Les cas présentés dépendent des besoins pédagogiques de la session

- Plan d'orientation sécurité, schéma directeur ISO 2700X, ISO 27001 appliqué au Contrôle d'accès IAM ; cartes professionnelles de santé (CPS) ; sécurité logique des applications sensibles; le PCA ; Sécurité Intranet pour des serveurs CITRIX connectés à des terminaux passif ; Sécurité des micro-processeurs nomades ; Contrôle des risques dans la production et le stockage des produits de santé ; Sécurité d'un réseau ouvert ; sécurité d'un dispositif de télé médecine (téléconsultation à distance, H2S)

Certification

Le processus de certification est innovant et issu de la collaboration entre le Pole Santé de Centrale Paris et les responsables pédagogiques.

- Il est basé sur un travail concret, en groupe (4 à 5 élèves) :
 - Identification de cas concrets ou d'une analyse critique d'une situation
 - Sélection et construction d'un projet d'optimisation Risques/Qualité/Coûts (méthodes, ressources, modalités)
 - Réunion des conditions d'application de la solution choisie
 - Présentation des sources de progrès et améliorations potentielles

Le candidat peut alors être certifié par l'École Centrale Paris Executive Education.