Executive Education Pôle Santé

Les nouveaux défis de la qualité et de la sécurité des systèmes d'information en Santé et de la E-Santé (télémédecine..)

Les Bonnes pratiques en matière de qualité, de sécurité, et de continuité d'activité

Coordonnateurs :
Vincent Leroux et Paul de Kervasdoué

EN PARTENARIAT AVEC :

Commission GALIEN

Commission GALIEN : Ce Haut Conseil français pour la Télésanté et des coopérations francophones a été créé en décembre 2008 par 12 membres fondateurs. Cette instance reconnue et respectée compte à ce jour une quarantaine de personnalités de très haut niveau parmi les associations de patients, de professionnels de santé, d'industriels et de hauts fonctionnaires. L'objectif de la Commission Galien est simple dans l'énoncé : *faire de la France un leader mondial de la télésanté au service d'une prise en charge équitable des besoins sanitaires de tous nos concitoyens*. En jouant, en tant que de besoin, un rôle de puissant aiguillon.

Contact : Ghislaine ALAJOUANINE –Présidente
presidente@galientelesante.org – 33 (0)6 09 17 93 02

GIXEL

GIXEL : (Groupement Industriel de l'interconneXion et des systèmes Electroniques – www.gixel.fr), membre de la Fédération des industrie électriques, électroniques et de communication (FIEEC) réunit les industries spécialisées dans les composants et dispositifs électronique embarqués ou implantés dont l'objectif est de stimuler dynamique industrielle des nouveaux marchés, en particulier eu égard aux besoins des membres de l'Union européenne.

Contact : Michel SCHALLER – Vice Président
michel.schaller@thalesgroup.com – 33 (0)6 60 45 62 29

LESISS
Les Entreprises des Systèmes d'Information Sanitaires et Sociaux

LESISS (Les Entreprises des Systèmes d'Information Sanitaires et Sociaux – www.lesiss.org), également membre de la FIEEC a été créée en 2005 avec une trentaine d'entreprises. Aujourd'hui composée de plus de 90 adhérents, LESISS regroupe les industries des technologies d'information de santé et pour l'aide à la personne. Grands acteurs internationaux et PME expérimentées s'y côtoient afin d'élaborer les outils qui permettront une disponibilité équitable du système de santé pour tous les français et la réduction de la fracture sanitaire.

Contact : Yannick MOTEL - Délégué général
ymotel@le6.org – 33 (0)6 30 40 20 36

PROBLEMATIQUE

De nombreux objectifs apparaissent pour les professionnels de Santé et les directions des systèmes d'information dans le vaste domaine de la santé :

Bâtir une analyse de risque globale, liée à l'usage des systèmes d'information, de l'informatique et des télécoms. En pratique recherche des : Pertes directes, Pertes Indirectes, Gravité, impact et probabilité de survenance. Détermination de l'Assurance Perte d'Exploitation Informatique et RC médicale, cartographie des risques et des scénarios de menaces (accident, erreur et malveillance) …).

Conduire un audit de sécurité informatique et télécoms ISO 2700X ayant pour cible un périmètre santé. En pratique : Questionnaire, progiciel d'audit, référentiel et résultat

Choisir et intégrer dans un système d'information un progiciel applicatif sur et de qualité,- Intégrer une nouvelle technologie : Rfid, logiciel embarqué, robot ou une nouvelle pratique ou un chemin d'accès clinique pour la téléconsultation clinique par exemple, ..) dans le système existant. En pratique : retour d'expérience, label HS2 (haute Sécurité Santé).

Identification et contrôle d'accès du personnel de santé, des patients et des biens. En pratique : maîtrise des 3 critères d'identification, traçabilité humaine et contrôle d'accès au système d'information, identitovigilance.

Continuité de service et d'activité dans l'offre de soins et traçabilité (preuve et contrôle). En pratique : Plan de continuité, en cas de sinistre : catastrophe naturelle, panne et malveillance et en cas de pandémie. Cela inclut la maintenance en condition opérationnelle (MCO) et la gestion de crise.

Sécurité du réseau informatique interne et externe. En pratique : maîtrise des solutions de sécurité TCP/IP : Internet, Intranet et Extranet, messagerie personnelle et professionnelle.

Connaître les coûts de la sécurité, réduire les coûts cachés et la non qualité. En pratique : exposer les critères pour calculer le Retour sur Investissement (ROI) lié à la sécurité d'un système d'information.

Identifier, valoriser et protéger le patrimoine informationnel : EPP, procédure de santé, recherche clinique, e-learning..

Bâtir une unité d'informatique thérapeutique dans un système d'information. En pratique : retour d'expérience, indicateurs de qualité et de sécurité dans le périmètre d'un Schéma Directeur de Sécurité du Système d'Information (SDSSI).

Aspects juridiques de l'usage de l'informatique en matière de soins médicaux (la preuve par e-mail, tierce partie de confiance et archivage des e mails…).

Nous sommes à un moment singulier : l'informatique pénètre « partout ». L'Internet change la réalité de la Santé. Nous modifions notre système de santé avec l'introduction de bouleversements en termes de gouvernance. Des projets de réseaux ou de pôles de Santé se multiplient dans toutes les régions et pour toutes les pathologies. Ils ont pour objectifs principaux de faciliter la communication et la coordination entre des professionnels de santé, ou du domaine social, dans un territoire donné. Des programmes de Dossier Patient et de gestion de la connaissance accompagnent ces organisations et ou ces établissements de santé.

La production de soins, la prévention, l'enseignement et la recherche médicale et scientifique, le développement industriel, la gestion et le contrôle des systèmes sanitaires et sociaux, se fondent sur la disponibilité au moment voulu, à l'endroit précis d'une information fiable pour les seuls opérateurs habilités. « La bonne information au bon moment pour la bonne personne dans le bon programme de santé »

Cette contrainte est confrontée en permanence avec le respect de la personne humaine et de ses droits de citoyen. Cela prend en compte le développement de la liberté individuelle et de la responsabilité du patient et du professionnel de santé.

Et nous percevons une évolution profonde de notre environnement informationnel, avec, dans le même temps, une difficulté à nous le représenter. Ces difficultés sont aggravées par la rupture que provoquent les technologies de l'information vers lma dématérialisation comme l'Internet, les cartes de Santé, le dossier personnel informatisé, le DMP, le logiciel embarqué sur un microprocesseur, la RFID… « L'information, constitue à la fois une ressource collective et une ressource individuelle » autrement dit un patrimoine informationnel.

Or, les technologies utilisées dans ces réseaux représentent de réels risques et des fragilités:

- Existence de dispositifs de piratage en libre service sur l'Internet ;
- Atteintes au patrimoine informationnel de l'établissement de santé ;
- Virus transmis en pièce jointe dans les messageries personnelles et professionnelles,
- Saturation des systèmes par l'envoi de messages répétés (bourrage) ;,
- Usurpation d'identité facilitée par la dématérialisation etc.,
- Les flux financiers transportés par les réseaux (paiement d'actes, feuilles de soins électroniques,...) et la confidentialité des données médicales propres à une personne.

Les menaces sont d'origine naturelle ou accidentelle, humaine, volontaire ou involontaire. Plus de 75% des préjudices informatiques ont pour origine le facteur humain, avec pour causes des accidents, des erreurs ou malveillances. Il en résulte un état de vulnérabilité qui affecte non seulement le système informatique et ses informations, mais encore l'image du professionnel de santé et de l'institution à laquelle ce dernier appartient.

Or, Les professionnels de santé (directeur, médecins, pharmaciens, etc…) doivent acquérir de nouveaux comportements.
S'il a pour son activité, classiquement une obligation de moyen, il est soumis pour son système d'information à une obligation de résultat en matière de continuité de service. « La qualité et la sécurité de l'informatique participent à la qualité et la sécurité des soins et de la prise en charge ».

PROGRAMME

Cycle de 16 jours répartis en 6 modules,

1 - Cible, périmètre objectifs et concepts de base de la qualité et de la sécurité du système d'information en matière de santé.

2 - Droit et assurance en matière de qualité et de sécurité du système d'information de santé.

3 - Méthodes d'analyse de risque, de diagnostic, de sécurité informatique et télécoms

4 - Les Produits, les réseaux et les services

5 - Mécanismes – mise en œuvre des méthodes – Cas pratiques – Retour d'Expérience.

6 - Examen pratique et certification.

OBJECTIFS

- S'approprier et mettre en œuvre dans les organisations de Santé, les méthodes et outils de gestion de la qualité et des risques en matière de technologies du système d'information
- Comprendre les liens entre qualité et la sécurité du système d'information et la qualité et la sécurité des soins et de la prise en charge
- Etablir et maintenir en condition opérationnelle un plan de continuité d'activité.

Intérêts pour le management d'un établissement :
- Former un responsable Sécurité des Systèmes d'information (RSSI) et mettre en cohérence avec le Gestionnaire des risques de l'établissement et la gouvernance globale.
- Former à la gestion de la qualité sécurité des systèmes d'information le Gestionnaire des Risques ou le Responsable Qualité.
- Accompagner l'informatisation des projets cliniques pour répondre à l'expansion de la e Santé (télémédecine) et la gestion de la connaissance et ainsi renforcer les méthodes de risque projet.

PARTICIPANTS CONCERNÉS

- Directeurs d'établissement, direction SI, RSSI, gestionnaire des risques médecins, Présidents de CME, DIM
- Cadres des ARS, de l'Assurance Maladie
- Industriel de l'informatique de Santé
- Toute personne intéressée par le management hospitalier et la sécurité informatique et des systèmes d'information en Santé.

MÉTHODES PÉDAGOGIQUES

Formation concrète basée sur l'exposé de méthodes reconnues, des études de cas, des conférences, une mise en application pratique.

Un travail de groupe (4 à 5 personnes) est organisé entre les séances pour des études de cas concrets et des retours d'expérience.

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) :

- L'identification de cas concrets ou d'une analyse critique d'une situation
- la sélection et construction d'un projet d'optimisation Risques/Qualité/Coûts (méthodes, ressources, modalités)
- la réunion des conditions d'application de la solution choisie
- la présentation des sources de progrès et améliorations potentielles

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

RESPONSABLES PÉDAGOGIQUES

M. Vincent LEROUX, Médecin de Santé Publique, Professeur à l'Ecole Centrale Paris, 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, ancien DSI, enseignant ECP.

TABLEAU PREVISIONNEL DES COURS ET DES CAS PRATIQUES

Module	Intitulé	Jour
1	**Cible, périmètre, objectifs et concepts de base**	
1.1	Concepts, Cible et périmètre de la sécurité informatique et télécoms en santé	0,5
1.2	Périmètre des systèmes d'information et des STIC en Santé	0,5
1.3	Organisation de la sécurité et de la qualité de la eSanté (HS2, ..) en France	0,5
1.4	Organisation des STIC en Santé, les agences (ASIP, Afnor…)	0,5
1.5	Risques et sécurité informatique des industries de santé (Laboratoires pharmaceutiques, éditeurs de logiciels compris)	0,5
1.6	Gouvernance des risques en matière de santé (place du RSSI/DSIO)	0,5
1	Sous Total	3J
2	**Droit et assurance en matière de qualité et de sécurité du système d'information de santé**	
2.1	Le droit en matière de sécurité dans le domaine de la santé : Droit des patients, CNIL, Charte de Cyber surveillance, droits d'auteurs	0,5
2.2	Responsabilité civile contractuelle et limites avec la Responsabilité délictuelle en Santé	0,5
2.3	L'assurance Perte d'Exploitation Informatique pour financer la reprise informatique après une panne ou un sinistre.	0,5
2.4	Sécurité informatique et aspects juridiques, contractuels de la sous-traitance	0,5
2	Sous Total	2 J
3	**Méthodes d'analyse de risque, de diagnostic, de sécurité informatique et télécoms**	
3.1	Plan d'orientation Sécurité ou Schéma Directeur ISO 2700X	0,5
3.2	Audit ISO 27001 – Identification (IAM) et Contrôle d'accès physiques et logiques, identitovigilance	0,5
3.3	Analyse de risque et évaluation de la sécurité des produits sensibles : cartes CPS, cles USB Firewall etc. Common Critéria ISO 15408 – Approche technico-commerciale	0,5
3.4	Analyse de risque des TIC des industriels des produits de santé	0,5
3.5	Sécurité des applications informatiques – et sous traitance Cloud Computing	0,5
3.6	La sécurité d'un réseau Intranet, Extranet Internet en santé	0,5
3.7	Bâtir un plan de continuité d'activité (PCA) en informatique de soins – Théorie et future norme BS 25999	0,5
3.8	Archivage traçabilité des données numériques (dossiers médicaux au sens large)	0,5
	Sous Total	4J

4	**Les produits, les réseaux et les services**	
4.1	Sécurité des réseaux numériques appliquée aux réseaux, établissements de santé	0,5
4.2	La sécurité des cartes santé : Contrôle d'accès, badges, Vitale et CPS	0,5
4.3	La sécurité des produits télécoms	0,5
4.4	Sécurité d'un réseau de soins ouvert	0,5
4.5	Qualité et sécurité des contenus : dossiers patients, moteur de recherche, Internet, HoNcode, netscoring..	0,5
4.6	Management opérationnel du DSI/RSSI Attaques Internet, gestion des personnels	0,5
4	Sous Total	3 J
5	**Mécanismes – Mise en œuvre des méthodes – Cas pratiques – Retour d'Expérience**	
5.1	Cas pratique : Plan d'orientation sécurité ou schéma directeur ISO 2700X	0,5
5.2	Cas pratique : ISO 27001 appliqué au Contrôle d'accès IAM – cartes professionnelles de santé (CPS)	0,5
5.3	Cas pratique : sécurité logique des applications sensibles	0,5
5.3	Cas Pratique : le PCA	0,5
5.4	Cas pratique : Sécurité Intranet pour des serveurs CITRIX connectés à des terminaux passif – Sécurité des micro-processeurs nomades..	0,5
5.5	Cas pratique : Contrôle des risques dans la production et le stockage des produits de santé	0,5
5.6	Cas pratique : Sécurité d'un réseau ouvert	0,5
5.7	Cas pratique : sécurité d'un dispositif de télé médecine (téléconsultation à distance, H2S)	
5…	….	
5	Sous Total : en règle 7 études de cas sont présentées en séances parmi les propositions et sont reparties durant les modules 1 à 4)	3,5
6	**Examen : Cas pratique de groupe**	0,5

MODALITES DE PARTICIPATION

Tarifs *(déjeuners et pauses offerts)*

- Cursus complet : 6 500 € HT (Certification incluse – 1 passage)
16 jours > 112 h
ou
- Possibilité de s'inscrire à un ou plusieurs modules sans certification :
1 000 € HT par module

Dates *(susceptibles d'être modifiées)*

de février 2010 à juin 2010

Cycle de 16 jours répartis en modules,
de 2 à 4 jours pour être compatible avec une activité professionnelle

Lieu : Paris ou Châtenay Malabry (92)

Inscriptions

Merci d'envoyer le bulletin et votre CV par fax (01-46-83-92-99) ou mail (info@cf.ecp.fr)

Attention : le nombre de places est limité, nous prenons les inscriptions en fonction de la date d'arrivée du dossier complet (bulletin d'inscription + CV)

Informations

Nathalie Glaziou
Tél. : 01 41 13 14 05
E-mail : info@cf.ecp.fr – www.cf.ecp.fr

Développer un programme « sur mesure », nous consulter