© Carole Derré

→ LE MANS, 20/22 AVRIL 2011

PREMIER CONGRÈS NATIONAL

Sécurité des Systèmes d'Information de Santé

Un congrès à la mesure des enjeux de santé publique

LIVRET SCIENTIFIQUE DU CONGRÈS

Le Mans Une Marque

Le Mans Métropole Communauté urbaine

LE MANS DEVELOPPEMENT

DSiH

Congrès national de la Sécurité des Systèmes d'Information de Santé

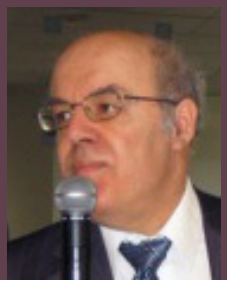
SOMMAIRE

Les partenaires

Organisation

l'agence Modeste

modeste@modeste.com
35 rue de Hauteville 75010 PARIS - Tél. : 01 47 70 55 97
1 place des Ifs 72015 LE MANS CEDEX 2 -
Tél. : 02 43 61 03 58 - Fax : 02 43 75 37 34



Monsieur Gérard PELIKS

Security Expert - Cyber Security Center CASSIDIAN - an EADS COMPANY

"Vulnérabilités, menaces, modèles économiques des attaques sur l'information et moyens de les contrer"

Gérard Peliks est expert sécurité dans le Cyber-Security Center de CASSIDIAN (nouveau nom de la division Defense & Security de EADS). Il travaille depuis plus de 15 ans dans le domaine de la sécurité de l'Information et depuis plus de 30 ans dans l'Informatique. Il préside l'atelier sécurité de l'association Forum ATENA, dans lequel il organise de grands évènements autour de sujets techniques sur le futur de l'Internet et coordonne l'écriture de livres collectifs sur la sécurité de l'Information. Il est membre du conseil d'administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information et du comité de pilotage du mastère Intelligence des Risques de l'ISEP. Il participe au groupe sécurité de l'AFNOR.
Gérard Peliks est chargé de cours sur différentes facettes de la sécurité, dans le cadre de Mastères à Télécom ParisTech, Télécom SudParis, à l'ISEP et dans d'autres écoles d'Ingénieurs.

Résumé de l'intervention

Savez-vous que l'espérance de vie de votre PC en réseau, sans antivirus à jour, sans firewall personnel bien paramétré, n'est que de quelques minutes avant qu'il ne soit contaminé par un programme malveillant parmi les dizaines de milliers qui tournent autour ? Ces malwares cherchent des vulnérabilités qui sont autant de portes ouvertes sur votre PC et sur votre information, pour entrer et délivrer leur charge létale, et souvent ces programmes malfaisants agissent en toute furtivité. Savez-vous que le marché de la cybercriminalité est aujourd'hui estimé à plusieurs centaines de milliards d'euros par an ? Quelles seraient les conséquences si les respirateurs d'un hôpital ou autres équipements médicaux tombaient sous le contrôle à distance d'un pirate ? Si les dossiers des patients étaient subtilisés par des individus qui veulent rentabiliser leurs méfaits ? Des menaces bien réelles pèsent sur toute information dématérialisée, et en particulier sur les informations nominatives et confidentielles des patients et du personnel hospitalier détenues dans les systèmes d'information des établissements de santé.

Aux cybercriminels qui s'intéressent à ce genre d'Information pour en tirer des bénéfices financiers conséquents, par chantage ou malversations, il faut ajouter les menaces de sabotages qui peuvent concerner les installations industrielles des établissements hospitaliers de plus en plus connectés à l'Internet. Même quand un réseau est totalement cloisonné et isolé, il utilise souvent les mêmes protocoles que ceux de la toile mondiale, donc même un établissement hospitalier, non connecté à l'Internet, n'est jamais à l'abri des programmes malfaisants véhiculés par exemple par des clés USB. L'exemple des dégâts occasionnés par le ver Stuxnet affectant les centrifugeuses de l'usine d'enrichissement d'uranium de Natanz en Iran, bien sûr non connectées à l'Internet, est là pour le prouver.
Quand ces menaces se concrétisent par des attaques qui prennent pour cible des systèmes vulnérables, et tout système comporte des vulnérabilités, certaines pas encore connues donc votre poste de travail, sans correctifs, n'a aucun moyen de s'en protéger, les effets peuvent être dévastateurs, et entrainer de plus des conséquences civiles et pénales pour les dirigeants.
Cette intervention portera sur les modèles économiques d'attaques contre l'Information, celles, techniques, qui s'appuient sur des botnets (dénis de services distribués et SPAM), et celles qui profitent de la naïveté ou de l'imprudence des victimes comme le phishing et ses dérivés. Il sera évoqué les problèmes particuliers posés par le passage vers le Cloud Computing et les dangers auxquels sont exposés les systèmes de contrôle des infrastructures de type "SCADA".
Mais nous verrons que des contre-mesures existent pour diminuer le risque jusqu'à un niveau connu et accepté, sinon acceptable, et que la meilleure façon de limiter ce risque résiduel passe par la sensibilisation des utilisateurs qui constituent en fait le maillon le plus faible de la chaine de sécurité qui protège vos informations sensibles.

Monsieur Jean-François LOUAPRE

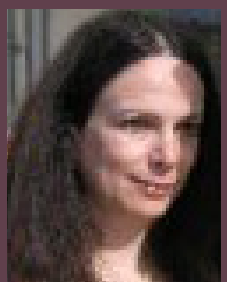
Responsable Sécurité - AG2R LA MONDIALE

"Démarches sécurité des SI dans la banque / assurance : l'âge de maturité"

Jean-François est le Responsable Sécurité du groupe AG2R LA MONDIALE. Il est en charge, outre de la sécurité des systèmes d'informations, de la continuité des activités du groupe et de la sécurité des personnes et des biens. Il a rejoint AG2R en 2007, en tant que RSSI, à l'issue de son parcours de 7 ans au sein de la Deutsche Bank, tout d'abord comme RSSI de la filiale française, puis comme coordinateur du programme de contrôle des risques informatiques pour 22 pays de la zone EMEA. Son expérience préalable de 10 ans a été acquise en sécurité informatique, système et réseau au sein de diverses SSII. Jean-François est également certifié CISM et ISO 27001 Lead Auditor, il participe activement aux travaux du groupe de travail NetFocus France et du Cercle européen de la sécurité des SI ainsi qu'à l'élaboration des manuels de préparation à la certification CISM (QAT de l'ISACA).

Résumé de l'intervention

Le secteur de la banque assurance est souvent perçu comme précurseur en matière de sécurité de ses systèmes d'information. Mais quels ont été les moteurs de la démarche de sécurisation des SI du secteur financier ? Les risques y sont-ils spécifiques ou peuvent-ils être généralisés à d'autres secteurs ? La démarche est-elle aujourd'hui stable et mature ? Quelles sont les "bonnes pratiques" généralement reconnues ? Au-delà de ces pistes de réflexion, la conférence vise au partage d'une expérience sectorielle mais potentiellement reproductible dans un environnement de santé.



Madame Mylène JAROSSAY
DSI Adjointe et RSSI – Institut Curie

"10 challenges spécifiques du RSSI Santé : méthodes et rôles du RSSI pour les atteindre"

Après quelques années en tant qu'ingénieur d'études et développement de protocoles et passerelles de communication chez un éditeur, puis en tant que consultante en architectures réseaux et télécoms au sein d'une société spécialisée dans le domaine de la Défense, Mylène Jarossay a rejoint l'Institut Curie, en tant que Directrice adjointe des Systèmes d'Information et RSSI.
Elle a contribué à l'élaboration d'un Système d'Information Hospitalier permettant la dématérialisation des données de santé à des fins d'optimisation des processus de soins et d'amélioration de la qualité des données et de la prise en charge des patients.
Dans ce contexte de données sensibles et critiques, sa mission RSSI s'est plus particulièrement portée sur la gestion des identités et des accès ainsi que sur la disponibilité de l'information et des applications médicales.

Résumé de l'intervention
Les RSSI Santé sont confrontés à des besoins de sécurité dans un contexte et avec des enjeux très spécifiques. Quels sont les principaux challenges qu'ils doivent relever et peut-on proposer des solutions et méthodes standard ? A travers deux mises en situation les intervenants vont s'attacher à illustrer ces challenges et les axes de travail pour y faire face

Monsieur Lazaro PEJSACHOWICZ

RSSI – CNAMTS et Vice-Président du CLUSIF

"10 challenges spécifiques du RSSI Santé : méthodes et rôles du RSSI pour les atteindre"

Très présent dans la vie associative des experts en Sécurité du Système d'Information, Lazaro Pejsachowicz est Vice Président du CLUSIF (Club de la Sécurité des Systèmes d'Information Français).
Il est Responsable de la Sécurité du Système d'Information de la Direction des Systèmes d'Information de la CNAMTS (Caisse Nationale d'Assurance Maladie des Travailleurs Salariés) poste qu'il a assumé en août 2002.
Il possède la certification PROCSSI et celle de "Lead Auditor ISO/IEC 27001".
Il a été chargé du cours d'Administration de la Sécurité à l'Université de Tours.

Lazaro est diplômé de la Faculté des Sciences Exactes de l'Université de Buenos Aires (Argentine) où il a suivi des études en Mathématiques et Informatique Scientifique. Il a débuté comme enseignant dans plusieurs Universités argentines (Buenos Aires, Olavarria, Lujan, UTN). Il a été informaticien en Suisse (ONU, Gènève) puis en France, dans des grandes Sociétés de Service en Ingénierie Informatique (Cap Sesa, Sema Group) principalement dans le domaine des Systèmes d'Autorisation Bancaires.
Par la suite il a exercé pendant plus de dix années chez Bull SA en tant que Responsable de la Sécurité et des Evolutions du Système d'Information de Bull Infrastructure et Système, avant de rejoindre, en 2001, France Telecom e-business, filiale FT dédié à l'hébergement de sites en tant que Responsable Sécurité des plates-formes.
Il a intégré en août 2002 la Direction Systèmes d'Information de la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés, en tant que RSSI.

Lazaro a participé à de nombreux séminaires et congres sur la sécurité en Europe et aux Etats Unis (Fraud & Security à Londres, Virus & Security à New-York, CISO Summit à Nice, Budapest et prochainement Madrid...).

Résumé de l'intervention

Les RSSI Santé sont confrontés à des besoins de sécurité dans un contexte et avec des enjeux très spécifiques. Quels sont les principaux challenges qu'ils doivent relever et peut-on proposer des solutions et méthodes standard ? A travers deux mises en situation les intervenants vont s'attacher à illustrer ces challenges et les axes de travail pour y faire face

Monsieur Yves NORMAND

RSSI et CIL - SIB

"L'approche des structures publiques de coopération hospitalière sur la sécurité des systèmes d'information de santé"

Yves Normand est Responsable de la Sécurité des Systèmes d'Information (RSSI) et Correspondant Informatique & Libertés (CIL) au sein du Syndicat Interhospitalier de Bretagne (S.I.B). Il intervient, depuis le début de sa carrière professionnelle, dans le domaine de la sécurité de l'information. Il a été Directeur Technique et Directeur Général d'une structure éditrice de solutions de sécurité (SSO, chiffrement de données...), pour le compte de banques, d'assurances et d'industriels. Puis, il a été consultant en SSI et chargé d'affaires, sur l'aspect organisationnel de la SSI (audit, analyse des risques, PSSI,...), pour le bénéfice de banques, ministères, DCSSI, collectivités territoriales.
Fort de la diversité de ses expériences, de son expertise méthodologique (EBIOS, normes ISO27000,...), de son écoute, Yves Normand intervient aujourd'hui pour les établissements de santé adhérents du SIB.
Yves Normand, ingénieur UTC, est certifié "Lead Auditor ISO/IEC 27001:2005", certifié "Risk Manager ISO/CEI 27005:2008", et membre de l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) - groupe de travail "Données de santé". Membre du groupe de travail "sécurité" de l'Asinhpa (association des structures d'informatique hospitalière publique autonomes).

Résumé de l'intervention

Les évolutions des pratiques métiers de l'hôpital, l'ouverture des systèmes d'information hospitaliers, les évolutions réglementaires (décret confidentialité, décret hébergeur, PMSSI,...) modifient la portée et la valeur de l'information.
La mise en réseau des établissements de santé, et notamment au sein des communautés hospitalières de territoire, et la convergence de leurs systèmes d'information sont devenues essentielles. La protection des données de santé des patients est primordiale.
Une démarche globale de management de la sécurité de l'information dans un établissement de santé est nécessaire et fondamentale. La Politique de sécurité des systèmes d'information (PSSI) et l'analyse des risques en sont des éléments fondateurs, ainsi que le plan de continuité d'activité (PCA).
Le SIB et le MiPih préciseront leur démarche d'accompagnement en sécurité de l'information pour leurs adhérents, ainsi que l'initiative des structures d'informatique hospitalière au travers du groupe sécurité de l'Asinhpa (association des structures d'informatique hospitalière publique autonomes).

Monsieur Christian ESPIASSE

RSSI et CIL – MIPIH

"L'approche des structures publiques de coopération hospitalière sur la sécurité des systèmes d'information de santé"

Le GIP MiPih structure de coopération inter-hospitalière a toujours mis au centre de ses préoccupations la protection des données du patient. La mission de Christian Espiasse s'inscrit dans cette perspective. RSSI en poste depuis plusieurs années il se charge de l'évaluation des risques, de la mise en œuvre et de l'application des mesures dans le but d'accroitre la sécurité des informations interne ou hébergés. Il a porté pour le MiPih le projet d'agrément en qualité d'hébergeur de données de santé obtenu le 17 mars dernier. Désigné CIL (Correspondant Informatique et Liberté) depuis bientôt deux ans il œuvre à la protection de la vie privée et des libertés individuelles au sein du GIP en veillant à la conformité des traitements de données personnelles. C'est aussi dans cette optique qu'il participe aux manifestations ou travaux sur les données de santé organisées par la CNIL ou l'AFCDP et qu'il collabore à l'élaboration de l'offre publique de référence dans le domaine de la sécurité du SIH.

Résumé de l'intervention

Les évolutions des pratiques métiers de l'hôpital, l'ouverture des systèmes d'information hospitaliers, les évolutions réglementaires (décret confidentialité, décret hébergeur, PMSSI,...) modifient la portée et la valeur de l'information. La mise en réseau des établissements de santé, et notamment au sein des communautés hospitalières de territoire, et la convergence de leurs systèmes d'information sont devenues essentielles. La protection des données de santé des patients est primordiale.

Une démarche globale de management de la sécurité de l'information dans un établissement de santé est nécessaire et fondamentale. La Politique de sécurité des systèmes d'information (PSSI) et l'analyse des risques en sont des éléments fondateurs, ainsi que le plan de continuité d'activité (PCA).

Le SIB et le MiPih préciseront leur démarche d'accompagnement en sécurité de l'information pour leurs adhérents, ainsi que l'initiative des structures d'informatique hospitalière au travers du groupe sécurité de l'Asinhpa (association des structures d'informatique hospitalière publique autonomes).

Madame Patricia THEBAULT

Expert Associée - Centre National d'Expertise Hospitalière
Chef du Service Informatique - Hôpital d'instruction Desgenettes - Lyon

"User d'un projet pour améliorer la sécurité : une nécessité…"

Expert associée depuis 2007 au CNEH, après une carrière en tant que Directeur de projets chez des éditeurs de logiciels hospitaliers, Patricia THEBAULT exerce également des fonctions de Responsable Service Informatique et Telecom au sein du Service de Santé des Armées.
Spécialiste des projets novateurs, elle conduit les changements d'organisation et l'optimisation des processus :
Former et conseiller sur le thème de l'identitovigilance depuis 2009
Améliorer la production des documents médicaux (reconnaissance vocale et secrétariats)
Optimiser l'organisation et la traçabilité des archives médicales
Rédiger le volet systèmes d'information des projets d'établissements
Son métier: Expertiser l'existant, conseiller et accompagner la maîtrise d'ouvrage des projets au plus près des professionnels de santé

Résumé de l'intervention
A l'heure des restrictions de budget et de la rationalisation des moyens, faire adopter une PSI et la mettre en œuvre est un défi. Si dans le quotidien nul ne songe à oublier d'assurer son habitation ou son véhicule, dans le domaine hospitalier, la notion de risque informatique reste un nuage flou encore trop souvent qualifié de paranoïa d'informaticien.
Le dialogue n'est donc pas aisé, et par voie de conséquence, les moyens financiers et humains très insuffisants. "Plaquer" une PSI et des mesures sécuritaires sur un système d'information déjà contraignant ne seront pas acceptées. Et comme toute contrainte, la première idée est de s'en libérer en la contournant.
C'est donc en empruntant la vision métier des acteurs de la santé que l'on peut créer des leviers permettant de générer un progrès dans la sécurité. Cette perspective doit s'inclure dans les projets mis en œuvre, comme un retour sur investissement attendu de chaque action amenant un changement.

Monsieur Bertrand BOUTELOUP

Président – 8i

"Les outils modernes au service de la sécurité des Etablissements"

Diplômé de l'Institut d'Administration des Entreprises de Rennes, Bertrand BOUTELOUP a débuté sa carrière à la Générale des Eaux au département des Cadres Hors Echelle. Sa première mission dans ce service "particulier" consistait en la migration d'un service de type BBS en une application de type Extranet. Après une année et demie de travail et le succès enregistré sur cette plate-forme qui deviendra l'Intranet Générale des Eaux, Bertrand est envoyé aux Etats Unis pour analyser le degré de sécurité des filiales nord-américaines et envisager le raccordement à la plate-forme Groupe. Il restera 6 mois à Boston avant de réintégrer la DSI du Groupe Générale des Eaux.
A la suite de cette première expérience, Bertrand fait un passage éclair chez Suez Lyonnaise des Eaux en qualité de Chef de projet Messagerie Intranet chez Lyonnaise Câble à Paris. Il arrivera pendant ces 6 mois à gérer le déploiement de la messagerie Lotus Notes sur l'ensemble des sites en France mais sa Bretagne natale lui manque.
C'est en 1998 qu'il retrouve ses terres de prédilection en rejoignant CAPGEMINI à Rennes en qualité d'Architecte Sécurité ; il restera dans cette entreprise 6 ans et occupera respectivement les postes de Responsable Practice Sécurité France, Responsable Practice Sécurité monde, Responsable du développement d'affaires Sécurité au niveau mondial. Ces années lui permettront d'approfondir ses compétences dans le domaine de la sécurité et de cultiver une vraie connaissance du développement des offres et de la gestion commerciale.
Après de longs mois de discussion, il accepte la proposition de UNISYS et prend la responsabilité européenne du développement des affaires sécurité.
Fin 2006, fort de ses 34 ans et de la connaissance du marché, Bertrand quitte Unisys pour créer sa propre structure,8-i, société spécialisée dans la sécurité informatique et l'identitaire. Cette structure compte aujourd'hui 31 personnes et est un des rares à avoir eu une démarche verticalisée dans le secteur de la santé.

Résumé de l'intervention

Dans un contexte où la menace et grandissante et où les vulnérabilités sont de plus en plus rapidement exploitables, de nouvelles technologies sont apparues afin de renforcer la sécurité de nos systèmes d'information. Ces nouvelles mesures ne doivent cependant pas contraindre les utilisateurs dans l'utilisation des systèmes d'information hospitaliers, les soins restant la priorité des personnels dans les hôpitaux.
C'est suivant ces deux axes que sont la sécurisation et le confort à l'utilisation que nous vous présenterons les nouvelles technologies à même de renforcer la sécurité globale des systèmes d'information et de fait, la sécurité des données des patients.

Ted Boyle

En traduction simultanée

"Privacy and Security Lessons Learned from an Operational Health Information Exchange"

Governments and care providers across the globe are investing in health information exchanges without fully understanding the privacy and security implications of broad scale electronic health record access. Lessons learned from NHS Scotland's fully operational HIE deployment could save the healthcare industry time, money and reputation.

Ted Boyle, joined the National Health Service, NHS, in 1996 after a successful career in the Royal Air Force. In 2001 he became responsible for the team of staff managing a Patient Administration System covering two of the United Kingdom's larger teaching Hospitals. During the next 10 years this system was updated to form a full Electronic Health Record. As a qualified Data Protection and IT Security Officer, Ted's responsibilities were widened to include all Information Governance issues arising from the use of EHR and HIEs. In all, the EHR holding 1.25 million records is used by 23,000 staff, in 4 major Hospitals, including the busiest ER in UK and at some 150 other locations across the South east of Scotland. He was also responsible for the audit of access to all the clinical applications as well as the security of the infrastructure which hosted the application. Ted now has his own consultancy specializing in Information Governance in the health arena.

Résumé de l'intervention
In the recent years with advances in technology there has been a drive in Europe, Canada, Asia Pacific and the United States towards an integrated Electronic Healthcare Record / Patient Healthcare Record (EHR / PHR) and introducing Health Care Information Exchanges (HIE). While the introduction of EHRs and HIE is at an early stage of maturity in many parts of the world the experience of implementation of an operation health information exchange in Scotland may provide guidance and considerations.
The benefits of EHRs and HIEs have been widely discussed and detailed in Clinical literature however, this presentation will consider the actual and unique privacy and security challenges in designing and managing a fully operational EHR and HIE. It addresses some specific security issues surrounding implementation, auditing of Patients and Staff and mitigating the insider threat.

Monsieur Nicolas CARPENTIER
Consultant Expert – ENOVACOM

"Quels arbitrages entre état de l'art technologique et pragmatisme opérationnel en matière de gestion des identités et des accès"

Nicolas Carpentier, ingénieur CNAM, est expert en architecture des systèmes d'information depuis plus de 10 ans. D'abord chef de projets J2EE et architectures distribuées au sein de la Web Agency Fi System puis chez l'éditeur BMC Software, il intègre ensuite le cabinet Cosmosbay/Solucom en tant que Consultant sénior. Après avoir mené pendant cinq ans des missions de conseil et d'assistance à maîtrise d'ouvrage notamment pour l'AP-HM, le CHRU de Lille, la CNAMTS ou le GIP-DMP, il rejoint en 2010 l'éditeur Enovacom. Aujourd'hui en charge de l'avant-vente et du marketing produit, il accompagne les établissements hospitaliers dans le déploiement de solutions de sécurité et d'interopérabilité.

Résumé de l'intervention
Il s'agit de présenter les solutions qui permettent aujourd'hui de faire progresser les établissements dans la maîtrise des accès aux données et applications métiers.
Comment une DSI peut-elle piloter l'évolution de son SIH en déployant des composants d'infrastructure qui répondent à ses besoins, tout en tenant compte de l'hétérogénéité des logiciels métiers ?
Comment structurer un projet de gestion des identités et des accès, quels sont les paliers pragmatiques atteignables en 2011 ?
Quels sont les facteurs clefs du succès de ce type de projet et quels en sont les principaux écueils ?
Quels sont les impacts des projets de rapprochement qui impliquent une mutualisation du SIH, comment partager de l'information au sein d'une communauté sans déconstruire l'existant ou ajouter une couche supplémentaire ?

Monsieur Nicolas MAQUET
Directeur Santé – ADVENS

"Médecins, soignants, administratifs, DSI…. Mieux gérer les risques de sécurité de l'information santé, ensemble"

Nicolas Maquet est Directeur Santé chez Advens. Il intervient comme consultant et coach dans l'élaboration ou l'optimisation de stratégies adaptées aux enjeux des établissements. Ces stratégies peuvent être globales aux établissements (rachats, contrôle de gestion et finances…), médicales ou autour de la sécurité de l'information et des risques associés. Ancien directeur de la polyclinique de la Louvière à Lille, puis directeur Régional Nord-Pas de Calais-Picardie-Champagne Ardennes-Normandie du groupe Générale de Santé, Nicolas Maquet dispose d'une connaissance approfondie du secteur de santé privé et public et GCS, de ses exigences et de ses enjeux. Il a été également conseiller du Ministre de la Santé pour la reconfiguration du secteur santé en Polynésie Française. Il est également intervenu comme expert-visiteur pour les certifications de nombreux établissements de santé V1, V2 pour la Haute Autorité de Santé.

Résumé de l'intervention
Les établissements de santé mettent en place des programmes coordonnés de traitements des risques : risques dans la prise en charge médicale du patient, risques d'infections nosocomiales, risques financiers et juridiques, etc. Mais cette gestion des risques ne prend généralement pas en compte la sécurité de l'information, considérée comme un sujet très technique et traité en mode purement réactif. Pourtant, certains incidents sur le SI d'un établissement peuvent avoir des impacts forts sur la prise en charge des patients, jusqu'à engager leur pronostic vital (impossibilité de réceptionner des appels d'urgence, erreurs ou délais dans les analyses biomédicales…). D'autres peuvent impacter grandement la capacité de l'établissement à équilibrer son budget (arrêt de la chaîne de facturation) ou exposer les données médicales.

Face à un SI qui s'ouvre et demande plus d'agilité (dossier médical partagé, informatique au lit du patient, télémédecine, mobilité…), il convient désormais de déterminer une approche globale, alignée avec la stratégie de l'établissement. Cette approche d'amélioration continue doit être sponsorisée par la direction, et doit associer l'ensemble des populations, médecins, soignants, techniques, administratifs afin de comprendre leurs enjeux majeurs. Elle doit viser à mettre en place une véritable gouvernance, basée sur la proactivité et l'anticipation dans les projets SI et les initiatives métiers, et la mesure des résultats.

Notre conférence visera donc à expliquer les leviers qui permettront de construire ensemble cette culture "risques" de sécurité de l'information, dans un écosystème encore peu conscient des impacts subis ou potentiels.

Monsieur Tristan SAVALLE
Directeur Sécurité - ADVENS

"Médecins, soignants, administratifs, DSI…. Mieux gérer les risques de sécurité de l'information santé, ensemble"

Tristan Savalle est Directeur Sécurité chez Advens. Il est notamment en charge de la définition d'offres à forte valeur ajoutée, adaptées au secteur de la santé et assure la direction de grands projets de sécurité pour différents clients. Il dirige actuellement un projet de mise en place d'un SMSI aligné ISO 27001 pour l'un des plus grands CHRU de France.
Tristan Savalle a commencé sa carrière au sein d'un grand cabinet de conseil Parisien où il a pu acquérir une vaste expérience dans le domaine de la sécurité de l'information auprès de clients "grands comptes". Il a notamment porté la réflexion autour des alignements et des certifications ISO 27001 et est l'auteur d'un livre blanc sur le sujet. Il porte des réflexions globales aux organisations, en collaboration complète avec les directions générales, les directions métiers et équipes support. Il est certifié CISSP et ISO 27001 Lead Auditor.

Résumé de l'intervention
Les établissements de santé mettent en place des programmes coordonnés de traitements des risques : risques dans la prise en charge médicale du patient, risques d'infections nosocomiales, risques financiers et juridiques, etc. Mais cette gestion des risques ne prend généralement pas en compte la sécurité de l'information, considérée comme un sujet très technique et traité en mode purement réactif. Pourtant, certains incidents sur le SI d'un établissement peuvent avoir des impacts forts sur la prise en charge des patients, jusqu'à engager leur pronostic vital (impossibilité de réceptionner des appels d'urgence, erreurs ou délais dans les analyses biomédicales...). D'autres peuvent impacter grandement la capacité de l'établissement à équilibrer son budget (arrêt de la chaîne de facturation) ou exposer les données médicales.

Face à un SI qui s'ouvre et demande plus d'agilité (dossier médical partagé, informatique au lit du patient, télémédecine, mobilité...), il convient désormais de déterminer une approche globale, alignée avec la stratégie de l'établissement. Cette approche d'amélioration continue doit être sponsorisée par la direction, et doit associer l'ensemble des populations, médecins, soignants, techniques, administratifs afin de comprendre leurs enjeux majeurs. Elle doit viser à mettre en place une véritable gouvernance, basée sur la proactivité et l'anticipation dans les projets SI et les initiatives métiers, et la mesure des résultats.

Notre conférence visera donc à expliquer les leviers qui permettront de construire ensemble cette culture "risques" de sécurité de l'information, dans un écosystème encore peu conscient des impacts subis ou potentiels.

Monsieur Christophe ADDINQUY

Directeur des Projets Back Office – VIDAL

"De la sécurité des systèmes d'information à la sécurité de la prise en charge : l'apport d'une base de données"

Christophe Addinquy, Directeur des Projets Backoffice VIDAL, a plus de 20 ans d'expérience dans le développement logiciel, auprès d'éditeurs et dans le conseil en nouvelles technologies. Il a ainsi mené à bien des missions de conseil, d'audit et de formation sur des sujets tels que la conception objet, la modélisation, le développement ou l'urbanisation des systèmes d'information. Passionné par son métier, il est très actif au sein de communautés professionnelles en marge de sa responsabilité sur le SI métier VIDAL. Il est actuellement membre du bureau des utilisateurs français de Scrum (sur les développements agiles), un sujet sur lequel il intervient régulièrement lors de rencontres.

Résumé de l'intervention

La sécurité des données médicamenteuses : les processus internes, du RCP à la donnée numérique.

La sécurité des données et l'intégration dans les logiciels métiers : évolution des outils

> Base de données à plat

> APIs et composants de sécurisation de la prescription

> APIs hébergées

La sécurité de la prise en charge : les outils d'assistance au paramétrage du livret thérapeutique.

Monsieur Nicolas CAUVET

Responsable Technique Editeurs – VIDAL

"De la sécurité des systèmes d'information à la sécurité de la prise en charge : l'apport d'une base de données"

Nicolas CAUVET est Responsable Technique Editeurs VIDAL. Avec plus de 7 ans d'expérience dans le développement de logiciels, Nicolas Cauvet s'est spécialisé de la gestion de projet AGILE. Au sein de la société VIDAL depuis 5 ans, il a la charge du développement des outils d'interfaçage. Il est référent technique auprès des éditeurs de logiciels.

Résumé de l'intervention

La sécurité des données médicamenteuses : les processus internes, du RCP à la donnée numérique.

La sécurité des données et l'intégration dans les logiciels métiers : évolution des outils

> Base de données à plat

> APIs et composants de sécurisation de la prescription

> APIs hébergées

La sécurité de la prise en charge : les outils d'assistance au paramétrage du livret thérapeutique.

Monsieur Frédéric ATTIA

Head of e-Health Skill Centers – ORANGE

"Que doit être un partenaire de confiance pour le monde la Santé ? avec un retour d'expérience sur le projet "Région sans film""

De formation médicale, titulaire d'un DEA de Science Technologie & Sociéte au CNAM et d'un Exec. MBA à l'Insead-Cedep, Frédéric Attia a mené sa thèse de doctorat sur les risques liés aux biotechnologies au Collège de la Prévention des Risques Technologiques à Matignon sous la Direction de JJ Salomon.
Il a ensuite été consultant dans la practice Santé d'Accenture avant d'intégrer la filiale Conseil de la branche Entreprise de France Télécom. Spécialiste des TIC et du secteur santé, il a ensuite crée sa boite de conseil pour l'industrie.
Il est actuellement Directeur du centre de compétence eSanté d'Orange Business Service pour la France et l'international et est responsable d'une équipe dédiée à la vente de solution IT et Santé pour la France. Il a été l'un des négociateurs du projet "Région Sans Film", une offre d'imagerie médicale partagée en commun entre Orange et Général Electric Healthcare en Ile de France.

Résumé de l'intervention
Hébergement des données de santé : bilans et Perspectives
Imagerie Médicale Partagée : retour d'expérience sur le projet Région Sans Film

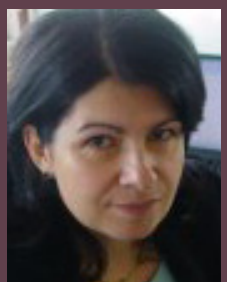
Monsieur Yves BLANCHET

Architecte en Chef du Secteur Santé et Sciences de la vie - IBM France

"Sécuriser les données médicales : panorama international des bonnes pratiques de sécurisation des données médicales au sein du SIH et en transit dans l'écosystème de santé"

Yves est Architecte en Chef du Secteur Santé et Sciences de la Vie d'IBM France.
Il a plus de 30 ans d'expérience dans les domaines du eBusiness, eAdministration, la dématérialisation des échanges, la sécurisation des échanges et de la Santé. Il a conçu des solutions de sécurité avancée liées à la mise œuvre d'un projet de dématérialisation du livre foncier. Yves Blanchet est diplômé de l'ENSI.

Résumé de l'intervention
La sécurisation des données médicales est une problématique commune aux établissements de santé des principaux pays développés, mais aussi de certains pays émergents. Un cadre règlementaire de protection des données personnelles médicales existe dans la plupart des pays démocratiques (HIPAA, Décret de Confidentialité, Volet "données médicales" des "Privacy Acts",..). Par ailleurs, la technologie permet de supporter l'introduction de nouvelles pratiques médicales prometteuses comme la télésanté, de nouvelles organisations en réseaux ou de nouveaux concepts comme les "clouds" médicaux. Toutes ces initiatives aboutissent au stockage et à l'échange de données médicales. L'angle d'approche de la sécurité informatique varie selon le degré d'avancement des projets de dématérialisation des données médicales et de leur échange. Ainsi, ceux qui utilisent déjà des solutions de dossiers patients électroniques renforcent la sécurité de leur système. D'autres développent de nouveaux systèmes de gestion de dossiers patients et d'échange de données médicales dans l'écosystème de santé, le tout "sécurisé dès la conception".



Madame Sophie TACCHI
Responsable des Offres Solutions de Sécurité – IBM France

"Sécuriser les données médicales : panorama international des bonnes pratiques de sécurisation des données médicales au sein du SIH et en transit dans l'écosystème de santé"

Sophie est Responsable des Offres "Solutions de Sécurité" d'IBM France depuis 18 mois et chez IBM depuis 1998.
Depuis 28 ans, elle s'est spécialisée dans la dématérialisation de l'argent, des valeurs mobilières et de la sécurisation des cartes d'identification et de transaction électroniques. Chez IBM, elle a initié et réalisé de nombreux projets de dématérialisation (B2B, B2C, A2C) chez les grands comptes d'IBM en France et dans d'autres régions du monde. Sophie Tacchi est diplômée de Paris-Dauphine.

Résumé de l'intervention
La sécurisation des données médicales est une problématique commune aux établissements de santé des principaux pays développés, mais aussi de certains pays émergents. Un cadre règlementaire de protection des données personnelles médicales existe dans la plupart des pays démocratiques (HIPAA, Décret de Confidentialité, Volet "données médicales" des "Privacy Acts",..). Par ailleurs, la technologie permet de supporter l'introduction de nouvelles pratiques médicales prometteuses comme la télésanté, de nouvelles organisations en réseaux ou de nouveaux concepts comme les "clouds" médicaux. Toutes ces initiatives aboutissent au stockage et à l'échange de données médicales. L'angle d'approche de la sécurité informatique varie selon le degré d'avancement des projets de dématérialisation des données médicales et de leur échange. Ainsi, ceux qui utilisent déjà des solutions de dossiers patients électroniques renforcent la sécurité de leur système. D'autres développent de nouveaux systèmes de gestion de dossiers patients et d'échange de données médicales dans l'écosystème de santé, le tout "sécurisé dès la conception".

Monsieur Pierre-Luc REFALO

Directeur Associé – HAPSIS

"La dimension socio-économique de la sécurité de l'information en santé"

Directeur associé du Cabinet de Conseil en Sécurité des Systèmes d'Information HAPSIS. En charge de l'activité "développement de la culture des risques informatiques et protection du patrimoine immatériel", il accompagne les Directeurs / Responsables Sécurité de grands groupes et de PME de tous secteurs d'activité. En 2011, il mène le projet de l'ARS des Pays de la Loire, visant à développer un processus d'acculturation à la protection de l'information médicale des SI de Santé.

Membre du Comité de Pilotage des Assises de la Sécurité (depuis 2003)

> Réalisation de l'enquête annuelle du Cercle Européen de la Sécurité
> Rédaction du Livre Bleu des Assises de la Sécurité
> Participation aux Assises de la Santé - Patronage du Ministre de la Santé et sous la présidence du Docteur Jean-Pierre Blum (Président de l'Institut International des Systèmes d'Information / Union Européenne et Directeur du Pôle Sécurité de la Commission Télésanté – Premier Ministre / Député Pierre Lasbordes).

Responsabilités antérieures

Entreprise (1997-2002)
> SFR/Cegetel : Directeur du Programme Sécurité de l'information

Relations institutionnelles (cybercriminalité, vie privée, signature électronique)
> G8
> Commission Européenne
> OCDE
> GBDe

Conseil / Service
> CISI (1989-1992)
> XP Conseil (1992-1997)

Enseignement et travaux associatifs

Membre actif
> Cercle Européen de la Sécurité (Groupe de travail Economie de la SSI)
> Clusif (Espace RSSI – 1998-2000)
> Cigref (Groupe de travail SSI – 1998-2002)
> ACSEL (Commerce électronique – 1998-2002)

Intervenant en formation professionnelle
> Université de Technologie de Troyes (Mastère SSI - depuis 2003)
> Ecole Centrale Paris (Certificat "Qualité / Sécurité des SI de santé" - 2010)
> ESIEE (Mastère IE - 2003-2007)
> Telecom Management (Certificat "Management de la SSI" – 2003-2009)

Résumé de l'intervention

Aspects socio-économiques de la Sécurité des Systèmes d'Information de Santé.
Depuis 20 ans, la sécurité des SI s'est concentrée sur les questions juridiques, méthodologiques et techniques. Dans tous ces domaines, une certaine maturité a été atteinte dans les secteurs de la banque / assurance, de l'industrie et des télécoms. Aujourd'hui, la prise en compte du facteur humain et la justification des dépenses sont des enjeux quotidiens pour les DSI et RSSI. Les liens avec les décideurs et les "métiers" se trouvent ainsi renforcés.
Pour sa part, le secteur de la santé doit rattraper un certain retard et est confronté à des enjeux majeurs liés à son cadre réglementaire (RGS, PGSSI, Décret confidentialité), à l'importance accrue des SI dans la qualité et la continuité de l'offre de soin et aux nouveaux usages liés aux projets comme le DMP, la bureautique / messagerie ou la télésanté.
S'appuyant sur les résultats des enquêtes du Cercle Européen de la Sécurité et sur des projets menés dans le secteur de la santé, cette intervention démontrera comment une approche socio-économique de la SSI est un facteur clé de succès des politiques et des projets "SI partagés de santé".

Monsieur Jean-Pierre THIERRY
Chief Medical Officer – AGFA HEALTHCARE

"PSSI et sécurité des patients : des enjeux nécessairement communs"

Jean-Pierre Thierry est médecin de formation. Il est actuellement le "Chief Medical Officer" de la société Agfa HealthCare qu'il à rejoint en 2007. En 2006 et 2007, il était chargé de mission dans les ARH de Picardie et de Nord Pas de Calais aprés avoir été pendant 4 ans DSI du CH Simone Veil (Eaubonne Montmorency) et du Centre Hospitalier Intercommunal de Créteil. Auparavant, en parallèle d'une activité de consultant dans le domaine des technologies médicales et de l'informatique de santé en France, Jean-Pierre Thierry a réalisé plusieurs études et expertises pour le compte de la Commission Européenne. Il est le co-auteur d'une étude sur l'apport des Système d'Information de Santé à la Sécurité des Patients pour la DG INFSO (eHealth for Safety, 2006).

Résumé de l'intervention
Le déploiement des Systèmes d'Information de Santé dans ses différentes composantes et plus spécifiquement le Système d'Information Clinique, est notamment justifié par la recherche d'une plus grande sécurité des soins. Le paradigme de la "Sécurité des Patients" permet en effet de situer les enjeux sanitaires : réduction des erreurs médicales évitables; recherche d'une meilleure efficience, par exemple grâce à des systèmes d'aide à la décision pour la prescription multimodale (CPOE) ; partage de l'information entre professionnels de santé d'un territoire ou d'une région (Dossier patient Partagé, Télémédecine, Télésanté, etc.) Dans ce contexte, la recherche du bon niveau de Sécurité des Systèmes d'Information représente une nouvelle problématique d'importance croissante compte tenu de la sensibilité des données traitées, des caractéristiques du marché de l'informatique de santé, de l'introduction de nouvelles techniques - mobilité, externalisation - et de l'évolution des réglementations au niveau national et international. Comme pour toute approche en matière de Gestion des Risques, l'investissement dans la Sécurité des Systèmes d'Information doit aboutir à garantir un niveau de risque aussi bas que raisonnablement possible compte tenu des facteurs économiques et sociaux. Dans le secteur médical, la recherche d'une balance bénéfice-risque doit impérativement tenir compte des objectifs d'amélioration de la Qualité et de la Sécurité des Soins.

Monsieur Eric GROSPEILLER

Fonctionnaire de la Sécurité des Systèmes d'Information - Ministère de l'Emploi, du Travail et de la Santé

"Gouvernance nationale de la sécurité des systèmes d'information de santé"

Eric Grospeiller, Fonctionnaire de sécurité des systèmes d'information rattaché au haut fonctionnaire de défense et de sécurité nationale, a notamment parmi ses missions l'orientation et le suivi de la mise en œuvre des politiques de sécurité des systèmes d'information pour les secteurs ministériels qu'il couvre. Ces politiques doivent être adaptées aux enjeux des établissements qui sont d'ordre opérationnels, en particulier pour assurer le fonctionnement nominal des systèmes d'information de santé et de protection sociale.

Résumé de l'intervention

L'évolution de l'offre de soin, avec pour objectif l'amélioration continue, repose en grande partie sur le développement des systèmes d'information. La garantie de la qualité et de la permanence de soins, tout comme la confidentialité légitimement exigée par les patients ou les professionnel nous oblige à prendre en compte la sécurité des systèmes d'information, avec un modèle de gouvernance approprié. C'est une des clé majeure de la réussite des orientations prises en matière d'hôpitaux numériques, de dossier médical personnalisé et bien évidemment de télémédecine ou d'e-santé.

Madame le Docteur Valérie SERRA-MAUDET

Chef de Service en Chirurgie - Centre Hospitalier du Mans

"Les Médecins et la PSSI peuvent-ils s'entendre"

Chirurgien depuis 1992, Praticien hospitalier depuis 1995, et Chef de service depuis 2009, Valérie SERRA-MAUDET est Vice-Présidente de CME de 2003 à 2010 puis devient Chef de Projet Médical sur le déploiement du Dossier Patient Informatisé au Centre Hospitalier du Mans, animant des groupes de Médecins et dirigeant la partie médicale du Projet.

Résumé de l'intervention

A la question "Les Médecins et la PSSI peuvent ils s'entendre ?", l'une des réponses est "Ont-ils le choix ?". Une autre peut être "Pourquoi ne le pourraient ils pas ?".

Celle choisie au CHM a été de parier pour un engagement commun et le développement d'un interprétenariat étroit. Comprendre et se comprendre, communiquer, "négocier", expliquer sont les maîtres mots d'un parcours nécessairement commun.

Monsieur Hervé SCHAUER

Chief Executive Officer – HSC

"Gestion des risques en sécurité de l'information dans la santé : illustration sur le DMP"

Hervé Schauer est un expert renommé internationalement en sécurité des systèmes d'information. Après des études d'informatique à l'Université Paris 6 (Jussieu), il s'affirme très tôt comme un des pionniers de la sécurité, informatique en France, avec (entre autres) la publication dès, 1987 d'une série d'articles sur la sécurité Unix et la détection, d'intrusion.
En 1989 il fonde son propre cabinet (Hervé Schauer Consultants). Il est l'inventeur du relayage applicatif (proxy firewall) pour l'agence française de l'espace (CNES) en 1991, présenté au Usenix Security Symposium en 1992, mais n'a pas brèveté son invention, ainsi celle-ci a été utilisée librement par la suite dans la majorité des firewalls commerciaux.
Hervé Schauer a publié ou contribué à de nombreux ouvrages et articles , notamment sur la sécurité Internet, le cloisonnement de réseaux, dont il est à l'origine, l'authentification, la sécurité des technologies sans fil, les normes ISO 27001 et ISO 27005, etc.
Hervé Schauer est conférencier invité et instructeur lors de nombreuses conférences spécialisées en Europe et au-delà.
Hervé Schauer a été consultant pour plus de 200 sociétés françaises et mondiales, des opérateurs de télécommunication, des gouvernements et des organisations internationales. Il est conseiller scientifique pour plusieurs start-ups, des entreprises établies et des sociétés de capital-risque.

Hervé Schauer a également des responsabilités dans de nombreuses associations, il anime notamment le groupe Sécurité Unix et Réseaux de l'OSSIR depuis 1989, a co-fondé l'OSSIR et les chapitres français de l' ISO et de l'ISSA, et a lancé le Club 27001 (chapitre français de l'ISMS Users Group).
Hervé Schauer est correspondant régulier sur la sécurité de l'information auprès de journalistes de la presse spécialisée.

Hervé Schauer est certifié CISSP par ISC2 (2004), ITIL Foundations (2007) et Information Security Foundation (2010) par EXIN, ProCSSI par l'INSECA (2004), ISO 27001 Lead Auditor (2005), ISO 27001 Lead Implementer (2006) et ISO 27005 Risk
Manager (2008) par LSTI, et QSA par le PCI-Council, et il a été enregistré ISMS provisional auditor par RABQSA (2007).

Résumé de l'intervention

Dans le cadre de la mise en œuvre d'un SMSI, l'appréciation des risques est un point fondamental, obligatoire, et la clé du succès dans la durée du SMSI. L'expérience d'un système unifié mais complexe dans la santé, où un des objectifs est la certification ISO 27001, a permis de voir où il fallait compléter les méthodes d'appréciation des risques existantes, comme EBIOS adaptée à l'étude d'un système en construction, et ISO 27005 conçue pour tourner dans la durée sur un système existant. Cette expérience a également permis de voir quel est le niveau de détail nécessaire, notamment quand celui n'existe dans aucun référentiel préexistant.

Docteur Yves LANNEHOA

ARS Pays de Loire

Comment intégrer la PSSI et ses outils aux contraintes médicales ? Comment impliquer les médecins dans la PSSI ?

Yves Lannehoa est Praticien Hospitalier Urgentiste au Centre Hospitalier Le Mans et chargé de mission pour la Collégiale des Urgences et des Soins Non Programmés en Pays de Loire. Il a été de 2003 à 2006 le coordinateur du groupe d'Informatisation des Urgences à la Société Française de Médecine d'Urgence, responsable de rédaction avec le GMSIH du livrable "Cahier des Charges National pour l'Informatisation des Urgences", soutien du déploiement National des Systèmes d'Information des Urgences. De 2005 à 2010, il a été correspondant pour l'Informatisation des Urgences en Pays de Loire, représentant au Comité Scientifique du Système de remontée des données Urgences pour la Veille Sanitaire. Il a, de 2008 à 2009 assuré la Chefferie de projet Fonctionnelle du dialogue compétitif pour le choix du Dossier Patient Informatisé du CH Le Mans. Il est par ailleurs Membre du Conseil d'Administration de la Société Française de Médecine d'Urgence, du Collège Régional de Médecine d'Urgence des Pays de Loire, et membre du comité de pilotage du projet LERUDI / prototype d'Outil d'aide à la consultation du dossier patient en situation d'urgence auprès de l'ASIP-Santé.

Monsieur Didier ALAIN
ANAP

Comment intégrer la PSSI et ses outils aux contraintes médicales ? Comment impliquer les médecins dans la PSSI ?

Didier ALAIN est Manager à l'Agence Nationale d'Appui à la Performance des Etablissements sanitaires et médico-sociaux. Il est également responsable du Master Management des Systèmes d'Information en Santé à l'université d'Angers. De double formation psycho-pathologie et systèmes d'information en santé, il a travaillé dans les hôpitaux pendant plus de 15 ans, sur des postes en charge de l'information médico-économique, en tant que responsable SI, puis pendant 5 ans à la tête d'une Direction des SI et de l'organisation. Il a également été consultant associé pour un éditeur de logiciel et a occupé les fonctions de conseiller national SI à la FEHAP. Passé à l'échelon national, il a est impliqué à l'ANAP depuis 3 ans sur le pilotage et la valorisation des investissements technologiques en santé. Cette approche l'a amené à s'interroger sur la destruction de valeur que peuvent potentiellement engendrer les TIC, aspects qu'il explore notamment dans ses fonctions universitaires.

Résumé de l'intervention

L'apport des technologies de l'information et de la communication (TIC) à la performance en santé reste un sujet largement polémique. Fonder un choix relève encore pour nombre de décideurs de la conviction, voire de la croyance, tant les référentiels, outils et éléments de preuve manquent. Pour autant, les publications sont particulièrement nombreuses et apportent un certain nombre d'éléments positifs, si ce n'est probants.

Se poser la question de la contribution des TIC à la performance des organisations de santé - autrement dit de la création de valeur par les TIC -, c'est également se poser la question de la destruction de valeur éventuelle, soit par absence de technologie (le risque "à ne pas faire"), soit par effet non maîtrisé de la technologie. Dès lors que les TIC supportent des processus critiques, leur impact peut être potentiellement vital pour les patients. L'informatisation de la prescription médicamenteuse est un exemple particulièrement frappant de ce point de vue. S'il est assez bien démontré que cette informatisation est positive du point de vue de la sécurité et de la qualité de la prise en charge médicamenteuse, ses effets indésirables ne sont pas ou peu discutés. La faible visibilité de ce sujet revient à pratiquer la politique de l'autruche, à un moment où la France connait une accélération importante de l'informatisation de la prise en charge médicamenteuse.

Un premier travail exploratoire, sur une base bibliographique, nous a permis d'identifier un certain nombre de sujets majeurs qu'il faudra impérativement traiter si l'on ne veut pas "jeter le bébé avec l'eau du bain" au premier accident grave qui sera médiatisé. J'en résume ici les grandes lignes :

- L'informatisation de la prescription médicamenteuse génère de nouveaux risques. Ces nouveaux risques ont des impacts potentiellement vitaux pour les patients, mais à ce jour, l'évaluation des impacts reste insuffisamment étudiée.
- Cette "e-iatrogénie" est un phénomène complexe et multifactoriel : nous avons en effet identifié que les causes racines relèvent de leviers éminemment différents, avec des populations et des univers professionnels qui sont rarement en dialogue ou en collaboration.
- Si les méthodes et les outils existent, leur mise en œuvre dans les projets en cours reste du domaine de l'exception, pour diverses raisons. L'HAS apporte une réponse importante, mais partielle par le référentiel de certification des LAP-H.
- Le nouveau risque généré par l'automatisation du traitement de l'information nécessite de créer des ponts entre les acteurs (en premier lieu entre les informaticiens et les médecins) et de former des compétences adaptées : face à la e-iatrogénie, la réponse doit être la création d'une nouvelle vigilance sanitaire : l'info-vigilance.

Monsieur Philippe STOPPA

FAIRWARNING

Comment intégrer la PSSI et ses outils aux contraintes médicales ? Comment impliquer les médecins dans la PSSI ?

Philippe Stoppa représente en Europe la jeune société FairWarning, basée aux USA, qui apporte des solutions innovantes dédiées aux établissements de soins pour protéger la vie privée des patients en collectant les traces des accès aux applications cliniques et médicales. Précédemment Philippe Stoppa a développé les marchés de la santé pour un leader de la sécurité des systèmes d'information.

François TESSON
e-santé Pays de la Loire

Comment intégrer la PSSI et ses outils aux contraintes médicales ? Comment impliquer les médecins dans la PSSI ?

François TESSON travaille depuis 12 ans dans le domaine de la sécurité des systèmes d'information (SSI). Titulaire d'un diplôme d'ingénieur Biomédical, il a assuré différentes fonctions dans le milieu de la SSI : Officier de la Sécurité des systèmes d'Information (OSSI) à la Délégation pour l'Armement (DGA), RSSI du CHU d'Angers et référent, au titre de l'ARH puis de l'ARS, des actions de SSI en Santé de la région Pays de la Loire. Il est à l'origine du Master Management des Systèmes d'Information en Santé à l'Université d'Angers dans lequel il est toujours actif. Il participe aujourd'hui activement à la création d'une structure dédiée aux systèmes d'Informations Partagés de Santé dans laquelle il apportera son expertise : «le Groupement de Coopération Sanitaire (GCS) e-santé Pays de la Loire». (e-santé Pays de la Loire favorise l'émergence, développe et la coordonne de nouveaux services de télésanté et de télémédecine en lien et à l'attention des professionnels de santé libéraux, des établissements sanitaires et des structures médico-sociales de la région.)

Résumé de l'intervention
e-santé Pays de la Loire s'est lancé dans une folle aventure : déployer un processus d'acculturation à la Protection des Informations Médicales des SI Partagés de Santé.
L'enjeu du projet est de faire adhérer les acteurs régionaux impliqués dans le processus de soins (décideurs, professionnels de santé, usagers, informaticiens ...) à la protection des données de santé afin que les usages intègrent efficacement les mesures de sécurité nécessaires. En particulier, le processus d'acculturation doit poser le socle indispensable à la bonne mise en œuvre des politiques de sécurité des systèmes d'information.
Cette acculturation doit aussi apporter une compréhension et un langage commun dans un domaine méconnu et parfois abscons.
L'objectif est clairement de changer les comportements, dans la durée, face aux défis de la numérisation de notre système de santé. Il s'agit de sensibiliser, d'informer et de former les personnes au bon moment avec les outils appropriés.

Monsieur Gilles TROUESSIN
SCASSI CONSEIL

Comment traduire le décret confidentialité en PSSI ? Quelle gouvernance pour la sécurité des données de santé ?

Après une thèse au CNRS (au LAAS – Laboratoire d'Analyse et d'Architecture des Systèmes) dans le domaine de la sûreté de fonctionnement et soutenue en 1991 sur le sujet du "traitement fiable de données confidentielles (par fragmentation-redondance-dissémination)", Gilles TROUESSIN a ensuite effectué un post-doc en 1992 à l'ONERA (au CERT – Centre d'Etudes et de Recherches de Toulouse) sur le sujet des "évaluations des propriétés de sécurité (par les théories de l'incertain)".
Ensuite, jusqu'en 2001, il a travaillé comme ingénieur d'études-sécurité à la CNAMTS au CESSI – Centre d'Etudes des Sécurités du Système d'Information, l'équipe qui avait conçu et développé la méthode d'anonymisation et la fonction FOIN – Fonction d'Occultation d'Informations Nominatives ; période durant laquelle il a été membre et animateur de groupes d'experts en "sécurité des SIS" pour la normalisation en "informatique de santé" ("health informatics"), à l'AFNOR, au CEN, à l'ISO.
Puis, de 2001 à 2005, il a rejoint le cabinet d'audit ERNST&YOUNG comme auditeur / consultant en Sécurité des Systèmes d'Information de Santé (SIS) et des Systèmes d'Information Hospitaliers (SIH), période durant laquelle il a conduit le projet de recherche : "Modèles et Politiques de Sécurité des Systèmes d'Information et de Communication pour la sphère Santé/Social (MPSSICSS – MP6)".
De 2005 à 2010, il a travaillé pour la Sté OPPIDA sud, comme consultant en sécurité des systèmes d'information de santé ; et s'est intéressé, à nouveau, à l'anonymisation et à la cohabitation entre les exigences de sécurité classiques incluant la confidentialité (ou confidentialité-discrétion) et les obligations de sécurité spécifiques incluant le respect de la vie privée (ou confidentialité-séclusion).
Depuis 2010, Gilles TROUESSIN a rejoint la Sté SCASSI Conseil, cabinet d'audit d'expertise et de conseil en sécurité de l'information où il est "responsable du département "sécurité des SIS / SIH"" ; Il est désormais très impliqué dans la protection des données sensibles (données de santé et/ou données à caractère personnel) ; en tant que adhérent et membre actif de l'AFCDP – Association Française des Correspondants à la protection des Données à caractère Personnel, il contribue à son Groupe de Travail "données de santé" et anime son Groupe de Travail Régional – Toulousain.

Thèmes d'intervention de Gilles Trouessin
Après plus d'une vingtaine d'activités dans différents domaines de la "sûreté de fonctionnement" (ou "dependability" en anglais), l'intervention de Gilles Trouessin lors de la table ronde "décret confidentialité et PSSI" et "gouvernance pour la sécurité des données de santé" consistera à informer / sensibiliser et à débattre / controverser autour des différentes facettes de la sûreté de fonctionnement, toutes aussi fortement concernées par la confiance justifiée et/ou justifiable que l'on serait en droit de placer dans les services rendus par les SIS en général et les SIH en particulier :
> sécurité-immunité ou "security" : via la disponibilité / intégrité / confidentialité / auditabilité ;
> sécurité-innocuité ou "safety" : éviter ainsi toute dérive vers une "informatique nosocomiale" ;
> fiabilité ou "reliability" : permettre aux systèmes de fonctionner sans risque de discontinuité ;
> maintenabilité ou "maintainability" : rendre aisée les maintenances évolutives/correctives ;
et par extension :
> intimité ou "privacy" : respecter la vie privée et protéger l'intimité de tout individu contre tout usage abusif ou illégal de ses données personnelles.

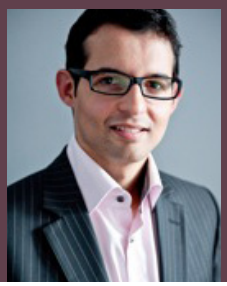
Résumé de l'intervention
En particulier, la table ronde de vendredi 22 avril sera l'occasion d'aborder les généralités mais aussi les spécificités de la SSI pour les SIS/SIH et, notamment, la complémentarité mais aussi la dualité entre la sécurité-security et la sécurité-safety, ainsi que les particularités et sensibilités nouvelles de la disponibilité, de l'intégrité et aussi de l'intimité-privacy dans le domaine de l'informatique de santé, à travers des questions stratégiques telles que :
> peut-on se contenter de PSSI standards pour protéger les S.I. de la sphère Santé / Social ?
> doit-on exiger des SIS / SIH qu'ils soient sûrs de fonctionnement ? Pourquoi ? comment ?

Monsieur Pascal VIOLLEAU

ENTERASYS

Comment traduire le décret confidentialité en PSSI ? Quelle gouvernance pour la sécurité des données de santé ?

Après des études d'ingénieur en informatique (SUPINFO), Pascal a fait ses premiers pas comme ingénieur réseaux au sein du laboratoire du Groupe Tests, puis comme architecte et directeur de projet réseaux et télécoms chez France Télécom. En 1999 Pascal a rejoint le groupe Bull où il a occupé des postes à responsabilité commerciale en particulier dans le secteur des grands comptes public, au sein de la division Réseaux et Sécurité. En 2008, Pascal Violleau rejoint les équipes Enterasys France et prend la responsabilité du pôle Public & Défense en ayant pour mission d'aider les partenaires d'Enterasys à commercialiser l'ensemble de la gamme de produits et solutions.



Maître Omar YAHIA

Avocat à la Cour

Comment traduire le décret confidentialité en PSSI ? Quelle gouvernance pour la sécurité des données de santé ?

Avocat au Barreau de Paris depuis 2005, et Associé au sein de la SCM SAINT MARC depuis janvier 2011, Maître Omar YAHIA a également été Juriste à l'Hôpital PAUL GUIRAUD VILLEJUIF, Responsable des affaires juridiques à l'Hôpital Privé Nord Parisien (SARCELLES). Il a également développé le département Santé du Cabinet DRAI Associés. Auteur de nombreux articles et chroniques en droit hospitalier et en droit de la santé (Santé RH, Finances Hospitalières, DSIH, etc.), il a créé en août 2006 un service d'information gratuit dénommé HOSPIDROIT, apprécié par les différents acteurs du monde sanitaire et social.

Résumé de l'intervention

L'organisation bien établie des archives hospitalières prévue jusqu'alors par l'arrêté du 11 mars 1968 a été durablement bouleversée par le décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel, lequel texte pose plus de difficultés pratiques qu'il n'en résout. La gestion des données invite à la plus grande prudence, le législateur lui-même hésitant à réglementer ce domaine, renvoyant ainsi les établissements à des instructions et des circulaires. L'intervenant fera le point sur l'état de la réglementation, du fait de la publication du décret n°2011-246 du 4 mars 2011, résultant de la loi HPST, et portant sur le contrat de prestation passé entre les établissements et les hébergeurs agréés.

Exemples d'articles (sur le dossier médical en lien avec les règles de conservation et d'archivage et le contrôle externe T2A)

http://www.hospidroit.net/archives/3399
http://www.hospidroit.net/archives/3336