Compte rendu de la deuxième réunion thématique du 23 septembre 2015

Sécurité Numérique en Santé, freins ou booster?

Invités

Jean-François Parguet (directeur technique et sécurité de l'ASIP santé)
Antoine Denis (Microsoft France - Responsable du développement des marchés Santé et Affaires Sociales).
Claude Champagne (Program Leader Data Privacy Europe, GE Healthcare)
Benjamin Sarda (Head Of Marketing, Orange Healthcare)
Pierre Desmarais (Avocat à la Cour – Correspondant Informatique et Libertés)

Les présentations sont disponibles en ligne sur les liens
http://www.telecom-paristech.org/#/group/sante/50/medias

http://fr.slideshare.net/TELECOM-PARISTECH-SANTE/edit_my_uploads

Etat des lieux

Les présentations ont permis de montrer l'étendue du problème de la sécurité numérique dans le monde de la santé. Cela va des instruments médicaux implantés aux infrastructures nationales d'échange et de partage des professionnels de santé en passant par les systèmes d'informations des hôpitaux et le PC du médecin libéral.

Systèmes informatiques

Les chiffres que donne Jean-François Parguet sont très révélateurs. Plus d'un million de professionnels de santé (en ne tenant compte que des 22 professions réglementées) et 60 000 structures de santé (dont 3000 établissements de santé) doivent pouvoir échanger des informations comme par exemple les 1,2 milliards de feuilles de soin électroniques traitées par l'assurance maladie.

Les acteurs de la sphère santé sont très sensibilisés à la confidentialité des données de santé à caractère personnel, mais ils ont une culture de la sécurité des systèmes informatiques assez peu développée. Ainsi seul 10 établissements de santé ont à ce jour généralisé l'utilisation de la Carte à Puce des professionnels de santé (carte CPS) pour se connecter au SI. L'hétérogénéité des terminaux avec des systèmes d'exploitation variés, souvent anciens, font qu'aucune politique de sécurité ne peut être mise en place sans une implication forte des utilisateurs. Imaginez les dégâts que peut faire un terminal corrompu sur un poste de travail de l'AP-HP qui gère de l'ordre de 15 millions de patients. Or les hôpitaux utilisent des systèmes de plus en plus sophistiqués qui fonctionnent avec de la télémaintenance comme nous l'explique Claude Champagne. GE Healthcare gère 120 000 équipements, dont 30000 connectés, dans plus de 2000 établissements en Europe.

Deplus le développement de l'hospitalisation à domicile et du déambulatoire fait que l'hôpital est obligé d'ouvrir son système aux réseaux publics. Makheureusement, comme l'explique Benjamin Sarda, la prise de conscience n'est pas réelle. Ainsi beaucoup de clients d'Orange utilisent les réseaux GSM 2G, sans authentification du réseau, pour échanger des données de santé. L'offre très sécurisée qui avait été bâtie pour l'HAD a été jugée trop chère par les hôpitaux.

Par ailleurs, le DMP devait jouer un rôle majeur pour la sécurité des données de santé. Ce projet sera repris par la CNAM.

La sécurité est trop souvent réduite à la dimension confidentialité alors que la disponibilité est tout aussi importante. Serait-il acceptable qu'un IRM présente un écran bleu pendant plusieurs heures, voire plusieurs jours? Ne pourrions-nous pas éviter des morts si les services d'urgence avaient l'information sur les allergies d'un patient ?

Et Jean-François Parquet de conclure qu'il faut avoir une démarche pragmatique de mise en œuvre de la sécurité dans les SI de santé. Il faut trouver un équilibre entre sécurité, performance et ergonomie. Il faut aussi savoir arbitrer entre confidentialité et perte de chance, et entre sécurité à priori (contrôle d'accès) et la sécurité a postériori (traçabilité).

Autres domaines

Mais les problèmes de sécurité numérique ne concernent pas uniquement les systèmes informatiques. Les objets connectés de santé sont des sources d'inquiétude. Les réactions des patients qui ont saturé les centres d'appel d'Orange suite à la série Homeland montre l'inquiétude des patients. Et le piratage d'un lecteur de glycémie connecté via Shodan nous démontre que ce n'est pas de la science-fiction.

Claude Champagne nous rappelle que la sécurité n'est pas un moteur mais plutôt une valeur intrinsèque du produit. La sécurité doit faire partie du produit pour avoir la confiance des clients. Or sans confiance, pas de marché ! Et Maitre Desmarais d'insister que la sécurité est un impératif car les patients n'acceptent plus le risque (cf. l'affaire Médiator).

Situation de la France

La sécurité doit être adaptée au risque qu'il faut donc évaluer. Aux USA la première cause de pertes de données de santé sont les attaques criminelles. Une enquête[1] a montré que 91% des sociétés interrogées avaient eu au moins un incident et le coût moyen des incidents est évalué à 2,1 M$. Au Royaume Uni, le premier secteur concerné par les pertes de données est de très loin la santé. l'Angleterre a mis en place un programme de certification de Gouvernance de l'Information (IGSoC) pour tous les acteurs de la santé.. Alors que la France est première ex-aequo avec le Brésil sur la probabilité d'attaque, il n'y a aucune publication sur les failles et sur les incidents.

Maitre Desmarais fait remarquer qu'il n'y a pas de plainte déposée pour violation des données de santé alors que les attaques des Systèmes d'Information sont quotidiennes.

Benjamin Sarda nous rappelle que la France s'est dotée d'un cadre réglementaire adapté, en particulier en encadrant l'hébergement de données de santé (article L.1111-8 du code de la santé publique, 4 Mars 2002) et en imposant un agrément (décret n°2006-6 du 4 janvier 2006). Cette démarche législative a été salutaire au début pour assurer la confiance. Mais le cadre Français n'est pas universel et au niveau européen, il est très difficile de travailler car contrairement aux USA les règles ne sont pas uniformes. Pire, il est très difficile de savoir ce qui se passe en Allemagne car la santé est gérée au niveau des Landers.

La démarche législative n'a d'intérêt que si les textes d'applications sortent rapidement. Par exemple, il semble que la loi de 1997 sur la prescription électronique ne soit toujours pas applicable faute de décret.

Par ailleurs, il faut avoir la volonté de faire appliquer les lois. Pourquoi l'adresse mail du médecin n'apparait-elle toujours pas suystématiquement sur les ordonnances des médecins français alors que c'est obligatoire en Europe pour permettre, par exemple, à un pharmacien allemand d'envoyer un mail au médecin Français.

Il faut aussi avoir des moyens crédibles de faire appliquer ces lois. Les 150 k€ d'amende infligés à Google ou la radiation du docteur Dukan sont risibles et

[1] Source Phonemon-ID experts 2015

discréditent les institutions sans être en rien dissuasifs. L'Europe travaille sur un règlement qui instaurerait des sanctions crédibles (1M€ ou 5% du CA). La France ferait bien de ne pas faire cavalier seul !

Le débat : Freins ou Booster

Maitre Desmarais propose la dichotomie suivante :

Frein	Booster
Sécurité = Investissement financier	Sécurité = avantage compétitif
Sécurité = Complexité technique	Sécurité = diminution de l'occurrence et de la gravité du risque + assouplissement en cas de défaut
Sécurité = UX délicate à vendre	
Sécurité = Frein au développement international	

Mais il précise que la problématique est plus complexe car dans le domaine de la santé, l'utilisateur attend un risque 0. Or la sécurité à 100% n'existe pas. En cas de problème nous risquons d'avoir une loi *Médiator* pour le numérique en Santé. La sécurité est donc un impératif qui doit être pris en compte par tous les acteurs.

Un premier consensus est que les industriels doivent considérer la sécurité comme une fonction indispensable des produits.

Un deuxième consensus est que la solution n'est pas dans les mains du législateur. En particulier, il est important que la France ne légifère pas toute seule. La législation Française incomplète et ambiguë a déjà des conséquences économiques importantes. D'une part, les grands industriels qui jouent sur le marché mondial se détournent du marché Français. Par exemple, Microsoft vend son carnet de santé électronique partout en Europe sauf en France. Or nous ne pouvons pas accuser Microsoft de vouloir piller l'Europe car ils sont en procès avec le gouvernement américain pour éviter de donner des informations confidentielles de leurs clients Européens. D'autre part, les start-up françaises dans le monde de la e-santé ne peuvent pas s'appuyer sur un marché national fort[2]. Si elles doivent respecter des normes françaises draconiennes, elles ne seront jamais compétitives à l'export et aucun investisseur ne voudra financer leur développement.

Nous avons eu l'information en temps réel que l'avocat général avait émit une opinion indiquant que selon lui l'accord Safe Harbour, qui permettait, sous certaines conditions de transférer des données personnelles en dehors de l'Europe, est invalide. (La Cour de Justice Européene a suivi d'un jugement le 6 octobre confirmant l'invalidité de Safe Harbour.) Notre sujet est donc

[2] Cf. Compte rendu de notre précédente réunion sur les modèles économiques en France

particulièrement d'actualité car l'Europe va devoir travailler sur le sujet. Il semble indispensable que les acteurs du monde de la santé définissent des normes et des standards.

Enfin si la sécurité numérique est nécessaire pour garantir la confiance des utilisateurs, ceux-ci sont des acteurs clef du problème. Une prise de conscience forte sur la sécurité est absolument nécessaire. D'une part cette prise de conscience est indispensable pour créer des modèles économiques vertueux. D'autre part, à quoi sert d'obliger les professionnels à stocker des données dans des data center certifiés santé si les applications qui sont utilisées, par exemple sous Androïd ou IOS, n'intègrent pas des règles de sécurité fortes pour éviter que les données ne soient instantanément stockées dans les cloud de Google ou Apple ? De plus la confidentialité ne garantit pas la validité de la donnée. Il y a un premier cas de poursuite en responsabilité dans le domaine de santé mobile concernant le suivi de grossesse. Le développeur s'est trompé dans le point de départ du délai d'IVG. La prise de conscience passe aussi par l'acceptation d'une part de risque. L'utilisateur doit arbitrer entre sécurité et perte de chance de soin.

Conclusion

La sécurité numérique en santé est un sujet très technique qui impacte beaucoup de domaines de la santé aujourd'hui. C'est un point critique pour le développement de la e-santé et pour la réforme du système de santé fondée sur le renforcement de l'ambulatoire.

La sécurité est nécessaire pour assurer la confiance des utilisateurs. Or sans confiance, pas de marché. Mais en retour, il est indispensable que l'ensemble des acteurs prennent conscience que la sécurité est impérative. Les industriels doivent considérer la sécurité comme une fonctionnalité clef de leurs produits. Les professionnels de la santé doivent accepter de respecter des règles. Enfin l'utilisateur final doit être conscient des risques et accepter de payer plus cher et d'intégrer la sécurité dans son comportement.

Une chose semble certaine, il est impératif de ne pas légiférer en France. La sécurité numérique est un problème global qui doit être traité au niveau de l'Europe. Compte tenu des délais de mise en œuvre, toute loi bride l'innovation et pénalise gravement l'industrie française, sans garantir la protection du citoyen.