techniques hospitalières

www.techniques-hospitalieres.fr

756
Mars-Avril 2016
71e année

Ambulatoire
Nuitée sur ordonnance
Trois circuits
Concepts architecturaux

Stérilisation
Impact d'un transfert de chirurgie
Dix ans du GCS Sterhospic
Qualification par acide peracétique

Jiqhs
Risque et performance au bloc
Mesure de la qualité en Suisse
Et nos données de santé ?
Démocratie sanitaire

Parcours patient
Et territoire
Et maladie chronique

Ingénierie biomédicale
Gestion des alarmes et monitoring

Support
Secrétariats médicaux

International
Innovations RH *made in USA*

SPH éditions
FHF FÉDÉRATION HOSPITALIÈRE DE FRANCE

Et nos données de santé dans tout ça ?

Objets communicants, homme augmenté, santé connectée : quel avenir pour nos données de santé à caractère personnel ? Comment penser la nouvelle confidentialité ? Quels moyens de sécurité seront-ils indispensables ? Gilles Babinet parle de l'ère numérique comme d'un « *nouvel âge de l'humanité* », et nous invite à « *penser l'Homme et le Monde autrement* ». Nous allons devoir repenser notre rapport à la donnée, quelle que soit sa qualité. Le professeur Guy Vallancien, dans *La Médecine sans médecins*, propose une vision prospective de la santé si réaliste qu'elle inquiète. Le *big data*, les *learning machines* qui diagnostiquent mieux que les docteurs, les dispositifs médicaux non plus « implantés », mais « embarqués » et bourrés d'électronique vont nous faire vivre plus longtemps en meilleure santé. Et la sécurité dans tout cela ? Quelles négociations allons-nous entamer avec le XXI[e] siècle pour fixer les clauses du contrat qui va nous lier, nous individus, au super-système ? Comment les espaces privés vont-ils se définir et pour quels usages ou objectifs ?

Vincent Trely
Président fondateur de l'Association pour la promotion de la sécurité des systèmes d'information de santé (Apssis), CEO du cabinet Proxima Conseil, membre de l'Association des réservistes du chiffre et de la sécurité de l'information (Arcsi)

L'essentiel

Si les technologies numériques vont avoir un impact positif sur notre santé, la question de la sécurité des données personnelles de santé ne s'est jamais posée avec autant d'acuité. Leur diversité et leur éparpillement, multipliés par l'apparition massive d'objets connectés de santé, rendent le contrôle de leur usage impossible à ce jour. Les intrusions dans les systèmes d'information des hôpitaux, peu préparés à la cyber-criminalité, se multiplient.

Mots-clés : données de santé ; SIH ; sécurité.

Les systèmes d'information de santé

La sécurité des systèmes d'information de santé est au cœur des débats depuis environ trois ans. Il était temps. Les technologies numériques offrent des révolutions positives dans nos existences, et le futur de notre santé en est parsemé. C'est donc non seulement certain du déferlement des technologies numériques embarquées, jusqu'en nous-mêmes, mais également optimiste quant à la capacité de nos sociétés à en séparer l'ivraie du bon grain que j'aborde mon propos. L'écosystème de santé est complexe. Parce que la santé n'est pas un processus industriel comme les autres, il possède une variable humaine majeure. Parce que le dicton « Honorez le médecin avant que vous n'ayez besoin de lui » perdure, on n'impose pas les choses au corps médical, on négocie. Parce que certaines pratiques médicales excluent *de facto* des pratiques usuelles propres à la sécurité numérique. Parce que les professionnels de santé sont peu acculturés aux concepts de la sécurité. Et parce que les instances nationales ont pris tardivement conscience de

la nécessité de lancer des opérations de sécurité dans ce secteur devenu très attractif pour les cyber méchants. Comment gérer un système d'information nécessairement communicant en assurant sa sécurité et le respect des libertés individuelles ? Comment envisager l'interconnexion de dossiers médicaux, de dispositifs technologiques (scanners, IRM, pacemakers et pompes à insuline connectés et pilotés à distance, dans le *cloud*), d'accès certifiés et de possibilités d'action par des milliers de profils utilisateur (du patient au médecin, des acteurs médicosociaux aux constructeurs d'objets et éditeurs de logiciels) au sein d'un espace de confiance ? Quels usages novateurs la cryptographie peut-elle apporter au système, en sus du chiffrement fort des données et des protocoles de communication cryptés entre les systèmes ? Les réflexions en cours sont abondantes et plutôt bien coordonnées : on trouve du réalisme technique et un travail de fond sur l'éthique ; la Cnil, le Cnom, le ministère, l'Anssi, l'Asip Santé, l'Anap[1] en sont les principaux producteurs. Les systèmes d'information de santé (SIS) sont en pleine mutation, impulsée par le programme Hôpital numérique, par les obligations de qualité des SI imposés par la Haute Autorité de santé (HAS), par l'obligation de mise en œuvre d'une politique de sécurité basée sur celle de l'État. C'est la troisième vague d'informatisation des établissements de santé, après les fonctions administratives et de support, puis les fonctions médicales avec les dossiers patients informatisés (DPI), les *Pictures Archiving and Communication Systems* (PACS), les progiciels de laboratoire, de prescription médicamenteuse, de blocs opératoires, de management des urgences… De grands projets régionaux et nationaux poussent cette modernisation, avec des progiciels en réseau, des messageries médicales sécurisées, des déploiements d'outils de télémédecine. Le développement massif de la chirurgie ambulatoire et le design des parcours de soin nécessitent la mise en réseau d'un ensemble hétérogène de professionnels de santé : médecins, hôpitaux, libéraux, pharmaciens, assistants sociaux, soins de suite et de réadaptation, maisons médicales, médecins spécialistes, psychologues… Le système est intrinsèquement communicant et cherche à l'être, quelle que soit la qualification des communications ! Le système n'est pas ignorant des technologies de l'information et de la communication et de leur constant développement alors il s'adapte et fait usage… Pour en rajouter, il est difficilement contraignable par l'essence même de sa mission. La complexité de l'ensemble est redoutable. La mise en réseau et la circulation de nos données de santé ne peuvent se faire que sous contraintes sécuritaires majeures. Et il y a, à ce stade, encore un long chemin à parcourir. Depuis 2012, la réalité parle et les prises de conscience se font, avec parfois un peu de brutalité. Regardons.

Deux mille quinze sera « *l'année du hack des hôpitaux* », prédisait en décembre 2014 la revue *MIT Tech Review*, en citant un chiffre qui ne manquera pas d'interpeller. Les intrusions dans les systèmes informatiques des hôpitaux auraient aug-

ATTAQUES INFORMATIQUES 2009-2013

Les exemples d'attaques informatiques d'établissements de santé se multiplient et, le sujet étant très sensible, beaucoup d'affaires ne sont pas ébruitées :

- **Hôpital américain en Virginie, mai 2009 :** vol de huit millions de dossiers médicaux. Intrusion d'un pirate dans le SIH et copie de 36 millions de prescriptions. Sauvegarde chiffrée restituée en échange d'une rançon de dix millions de dollars.
- **Centre hospitalier de Morlaix, juin 2012 :** saturation des réseaux. Accès internet coupé. Quinze jours pour le retour à la normale. En cause : infection par le ver Conficker *via* une clé USB.
- **Clinique de Champagne, juin 2012 :** plusieurs centaines de dossiers médicaux rendus disponibles sur Google. Demande de rançon d'un prestataire de services. Constitution d'une cellule de crise et retour aux dossiers papier. En cause : l'intervention hors contrôle d'un prestataire sur le poste d'un médecin.
- **Centre hospitalier de Saint-Malo, septembre 2013 :** mise en demeure par la Cnil pour cause de transmission de dossiers médicaux non anonymisés pour vérifier la cohérence du codage des actes. Plusieurs centaines de dossiers médicaux concernés. Image de l'établissement mise à mal.
- **Cinquante centre hospitaliers français, octobre 2013 :** fichier contenant identifiants et mots de passe et adresses IP des serveurs disponible sur internet. Possibilité d'intrusion et de consultation des dossiers médicaux. Erreur humaine du côté du fournisseur du logiciel de gestion des urgences.
- **CHU de Clermont-Ferrand, novembre 2013 :** vol de l'ordinateur portable d'un neuro-réanimateur. Dispositif antivol. Données de santé de patients, études scientifiques non encore publiées et non sauvegardées sur un autre support.

1- Cnil : Commission nationale de l'informatique et des libertés. Cnom : Conseil national de l'ordre des médecins. Anssi : Agence nationale de la sécurité des systèmes d'information. Asip Santé : Agence des systèmes d'information partagés de santé. Anap : Agence nationale d'appui à la performance des établissements de santé et médico-sociaux.

menté de 600 % depuis un an (selon les calculs de Websense, une agence de cybersécurité qui travaille pour le ministère de la Défense américain). « *Pour les organisations du monde de la santé, la question n'est pas de savoir si elles vont se faire attaquer, mais quand* », écrit Lynne A. Dunbrack, vice-présidente des recherches à l'institut IDC Health Insights et auteur du rapport 2014 sur les cybermenaces dans le secteur de la santé. Les pirates semblent s'être progressivement désintéressés des banques, aux systèmes informatiques trop complexes, pour se pencher sur les établissements de santé et les entreprises du secteur médical. Faute de moyens, ou de clairvoyance, ces derniers ont investi des sommes très modestes dans leur cybersécurité, constituant des proies faciles.

Les données médicales circulantes

Les systèmes numériques médicaux produisent des penta octets et bientôt des hexa octets (10^{18}) de données. Tout est stocké sur des infrastructures techniques complexes, virtualisées, redondées, parfois chiffrées. Celles-ci sont partout : au cœur des 1 200 centres hospitaliers français, des 7 000 établissements (Ehpad, USLD, SSR[2]…), des ordinateurs des médecins généralistes, des plateformes régionales ou territoriales de santé (dossier communicant de cancérologie, d'hématologie, d'imagerie…), mais aussi dans des applications médicales diverses, sur des plateformes variées, et autour des objets connectés ou communicants de santé. C'est un premier problème. La diversité et l'éparpillement des données, avec un contrôle d'usage impossible pour le moment. Tout va circuler, tout va dialoguer et calculer, pour notre plus grand bien-être. D'ici à vingt ans, nous aurons en moyenne une dizaine d'applications et d'objets communicants directement liés à notre santé, en mode gadget, dispositif médical ou « imposé » par notre mutuelle, voire par la Sécurité sociale, pour le calcul du bonus/malus lié à la prise en compte personnalisée de notre santé. Le marché du *big data*, c'est 60 % de croissance par an, avec 55 milliards de dollars prévus en 2016 par le Gardner Group et 4,4 millions d'emplois induits sur 2015-2016. Le business a donc démarré et le business n'est ni patient, ni philanthrope. On imagine aisément les conséquences potentielles de la création de systèmes de santé interopérants mal conçus ou mal sécurisés… Plus de 130 000 applications médicales sont disponibles en ligne dans les *stores*, des centaines d'objets connectés déferlent sur un marché mature et très attractif. Les nouvelles générations de médecins, qui ont grandi avec le numérique et sont avides de technologies, en font usage quotidiennement. Les systèmes d'information de santé vont devoir s'adapter rapidement, et rester robustes tout en accueillant l'irréversible modernité. La vigilance et l'acculturation des usagers, qu'ils soient professionnels de santé, patients ou simples citoyens, sont primordiales. La circulation massive d'images médicales pour avis ou diagnostic complémentaire *via* les réseaux de smartphones de tous constructeurs et tous opérateurs, hors de tout processus sécurisé, est un exemple de mésusage. L'usage intensif d'applications médicales issues des *stores* et utilisées par les jeunes médecins, hors de contrôle des directions informatiques, et sans avoir pris connaissance

ATTAQUES INFORMATIQUES 2015

- **Hôpitaux universitaires de Strasbourg, janvier 2015 :** le site internet des HUS a été « *piraté et infiltré* ». La page d'accueil a été remplacée quelques instants par un fond noir avec différentes inscriptions : « *Fallega Team, Tunisian Hackers* », « *Nik le groupe radio du Charlie* », « *Gr33tz : Les Muslman* » *(sic)*. Cette attaque informatique est liée aux actes terroristes perpétrés en janvier (plusieurs milliers de sites internet français ont été la cible d'attaques en provenance d'une mouvance islamiste).
- **Centre hospitalier de Châteauroux, janvier 2015 :** « *Nous avons constaté un ralentissement des ordinateurs* », raconte le directeur adjoint de l'hôpital. Selon lui, un virus aurait infecté les ordinateurs du centre hospitalier « *connectés à internet* ». Il s'agit de Trojan Kryptik, cheval de Troie qui a la capacité de crypter des données stockées. Le Samu serait resté injoignable pendant une quinzaine de minutes.
- **Labio, mars 2015 :** quelque 40 000 identifiants et des centaines de bilans médicaux et d'analyses sanguines se sont retrouvés entre les mains du groupe de hackers Rex Mundi, qui a exigé une rançon en échange de la non-publication de ces données. Face au refus d'obtempérer du laboratoire, les bilans non cryptés de 15 000 patients ont été divulgués sur internet, où ils sont restés consultables pendant plusieurs jours.
- **HAS, juillet 2015 :** le site de la Haute Autorité de la santé a subi une attaque informatique qui a porté préjudice à l'institution, mais aussi à plusieurs entités économiques françaises et à des centaines de Français. Le pirate s'est attaqué à la console qui gère l'espace de déclaration d'intérêts de la HAS.
- **Hôpital universitaire de Californie, mai 2015 :** des données médicales non chiffrées concernant 4,5 millions de personnes de la région ont été dérobées. La faille remonterait à octobre 2014 mais n'a été découverte que le 5 mai 2015. (Source : http://www.lemarson.com/actualite/567/l-hopital-universitaire-de-californie-pirate-pres-de-4-5-millions-de-personnes-concernees.)

2- Ehpad : établissement d'hébergement pour personnes âgées dépendantes. USLD : unité de soins de longue durée. SSR : soins de suite et de réadaptation.

> « Pour les organisations du monde de la santé, la question n'est pas de savoir si elles vont se faire attaquer, mais quand. » Lynne A. Dunbrack

des complexes conditions générales internationales des éditeurs, en est un autre. Les pacemakers peuvent être piratés et détournés pour délivrer des impulsions électriques mortelles. Il en est de même des scanners, IRM ou pompes à insuline. Ces « incidents » de sécurité, que l'on devrait parfois qualifier d'accidents, se multiplient. Si certains organismes choisissent l'axe de la transparence en en informant leurs clients ou usagers, combien choisissent celui du silence ?

Les objets connectés de santé

Pour ajouter à la complexité initiale, l'apparition rapide et massive d'objets connectés de santé et leur appropriation tant par les patients que par les professionnels de santé (**Annexe**), relance avec force le dossier sécurité, sous tous ses aspects – techniques, territoriaux, juridiques – et pose la question de la qualité du « DICP » (disponibilité, intégrité, confidentialité et preuve ou traçabilité). Objets de toutes origines, sociétés récentes et peu identifiées, conditions générales d'usage des éventuelles données collectées opaques, qualité du développement des applications inconnue, labellisation non opérationnelle : autant de questions cruciales qu'il est temps de se poser. Car la vague ressemble à un tsunami. Les marchés prévus en milliards de dollars, la moyenne de huit applications médicales ou de bien-être (*quantified self*) par personne pour les Anglo-Saxons et l'explosion du marché français prévue pour 2016 vont faire entrer certains de ces objets dans notre quotidien comme le smartphone ou l'aspirateur.

Fin de la confidentialité comme valeur

Albert Einstein prévenait : « *Le monde que nous avons créé est le résultat de notre niveau de réflexion, mais les problèmes qu'il engendre ne sauraient être résolus à ce même niveau.* » Il ajoutait : « *Il est hélas devenu évident aujourd'hui que notre technologie a dépassé notre humanité.* » Selon les études (Gardner et autres), il est attendu entre 80 et 210 milliards d'objets connectés à l'horizon 2020. Comment construire un usage sage, raisonné et conscient de ces nouveaux objets ? Comment classer ce qui aura un impact positif sur le parcours de soin et ce qui relèvera du gadget ? Comment les médecins vont-ils accorder, ou non, leur confiance à ces outils, et avec quelles garanties ? La nouvelle génération, s'en préoccupe-t-elle ? Et qui va payer ? Les réponses à ces questions essentielles vont fonder les modalités d'un usage pour longtemps, avec une irréversibilité évidente des options prises en début de processus. La philosophie humaine et l'évolution des sociétés vont également réviser de fond en comble le concept de confidentialité. Les nouvelles générations, et même les plus anciennes, abordent très facilement leurs problèmes de santé, sur les réseaux dits sociaux ou les forums spécialisés, laissant partout la trace de leurs pathologies ou de leurs petites souffrances quotidiennes. Ces données sont innombrables, produites chaque jour directement par les patients, conscients ou inconscients de dévoiler, entièrement ou par petites briques, leur dossier médical de façon quasi irréversible. Nos données personnelles circuleront, seront analysées, traitées, pour apporter en permanence les bonnes réponses à nos désirs. En ce qui concerne la santé, il en sera de même. L'objet connecté de santé est le dernier rempart avant le corps connecté, nouvel essor que nous préparent les nanotechnologues. Les micro-robots qui nous répareront en temps réel existent déjà au sein des programmes de nanorobotique. La sécurité de ces dispositifs et la confiance que nous serons prêts à leur accorder seront déterminantes dans leur développement. L'adhésion du corps médical est une nécessité, pour éviter de voir s'installer deux systèmes parallèles de diagnostic et de traitement, comme c'est aujourd'hui le cas avec la conservation massive de processus papier malgré l'informatisation. L'ignorance relative aux conséquences de l'usage est le principal débat et l'éducation des populations est la seule réponse connue. Nous avons tous une responsabilité à prendre et à assumer concernant notre avenir, la recherche de l'équilibre entre le bien et le mal étant toujours le cœur de la question. Je conclurai en citant Winston Churchill, qui disait : « *Mieux vaut prendre le changement par la main avant qu'il ne nous prenne par la gorge.* » Alors nous adhérerons, parce que c'est le progrès… ■