

Un enjeu stratégique pour l'hôpital

Les assises de la sécurité et des systèmes d'information qui se tiennent chaque année en octobre à Monaco ont accueilli pour la première fois un pôle santé. À l'heure où les hôpitaux investissent massivement dans les services informatiques, la sécurité de ces systèmes est devenue un enjeu stratégique.

DE NOTRE ENVOYÉE SPÉCIALE

INFORMATISER, c'est plus de sécurité (pour la prise en charge thérapeutique par exemple) mais c'est aussi prendre des risques. Et le risque, c'est le virus Conficker qui a paralysé plusieurs hôpitaux entre janvier et juillet dernier. Ce sont les attaques de « hacker » (pirate informatique) déjouées par le CHU d'Amiens ou par la plate-forme Emosis qui héberge les dossiers médicaux de Franche-Comté. Mais c'est aussi un service de néphrologie qui prend comme identification-mot de passe « *dialyse-dialyse* », histoire que tout le monde puisse s'en souvenir !

Même s'il est moins coûteux de l'intégrer au départ, la sécurité informatique n'a pas toujours été la priorité d'établissements dont la mission première est de soigner. Obsession des services informatiques, elle était même ressentie comme une entrave par les professionnels de santé. Le contexte a changé avec les plans Hôpital 2007 puis 2012 (en 2008, les dépenses informatiques du secteur de la santé ont dépassé 1,5 milliard d'euros) dont une large part est consacrée aux systèmes d'information, avec la perspective du dossier médical personnel (DMP) et les initiatives gouvernementales comme les directives nationales sécurité. L'arrivée de la télé santé va réclamer elle aussi une vigilance accrue. L'ANSSI (Agence nationale de sécurité des systèmes d'information) était présente pour affirmer que « *dans ce secteur d'importance vitale, les risques sont nombreux et interdépendants* ». Et l'ASIP (Agence des systèmes d'information partagés de santé) pour assurer qu'un guide de recommandations sécurité spécifique à la santé était en préparation.

Le club des RSSI hospitalier.

Sur le terrain, les directions informatiques (ou DSI) sont de plus en plus convaincues de la nécessité absolue du pilotage médical des projets. Surtout quand ils incluent la participation des soignants. Au sein du CHU de Besançon, les professionnels de santé effectuent 500 000 à 600 000 clics par jour. Un projet informatique doit rentrer dans le projet médical d'établissement et améliorer tant la pratique métier que la prise en charge du patient. « *La sécurité doit devenir une valeur à partager* », dit Pierre Thépot, directeur général du centre hospitalier d'Arras.

D'où l'apparition dans les hôpitaux (ou à un niveau régional) de responsables sécurité des systèmes d'information (RSSI). Manager du risque informatique, le RSSI assiste la maîtrise d'ouvrage, apporte son expertise sur la législation et sensibilise à la sécurité. Il cumule sa fonction avec celle de correspondant Informatique et libertés (en relation avec la CNIL). De huit membres l'an dernier, le club des RSSI hospitaliers est passé à une quinzaine en 2009. On y réfléchit notamment sur l'identifiant patient (IP) et le problème des appareils biomédicaux (voir encadré). « *On va remettre un livre blanc aux tutelles* », préviennent-ils.

Concrètement, la mise en conformité des établissements avec le décret confidentialité (voir encadré) relève de leurs compétences. C'est un gros chantier surtout pour les petits hôpitaux qui sont en train de se regrouper (MIPIH pour Midi-Picardie Informatique hospitalière, SIH Nord Pas de Calais fédérant 26 établissements).

24 hôpitaux mettent en œuvre la « CPS ».

L'usage de la CPS ou d'un équivalent est recommandé pour l'accès au SIH (système d'information

hospitalier). « *Vingt-quatre hôpitaux sont en train d'expérimenter son déploiement* », précise Marthe Wehrung, directrice générale du GIP-CPS qui vient de fusionner avec l'ASIP Santé. À l'hôpital psychiatrique Henry Ey de Bonneval, dans l'Eure, on a choisi la CPS (52 médecins et secrétaires équipées) et des lecteurs de cartes. Ce qui suppose de gérer les droits d'accès, de trouver une solution pour les oublis de carte et les stagiaires. Le CHU de Lille a préféré une carte sans contact qui gère aussi l'entrée à la cantine et au parking. « *Une étude montrant qu'un utilisateur se connectait 15 à 20 fois par jour sur le poste de travail*, explique Guillaume Deraedt, RSSI, *la CPS serait restée en permanence dans le lecteur. Le professionnel s'authentifie une fois avec sa carte dans le lecteur et il lui suffit ensuite de s'approcher du poste pour être reconnu* ».

C'est le principe du SSO (*Single sign-on*) : on ne s'authentifie qu'une fois par jour. Couplé avec l'utilisation de la CPS, c'est le mot magique dont l'utilisateur perçoit immédiatement l'intérêt... comme pour la traçabilité. « *Nous avons eu un dialogue avec les soignants*, se félicite Guillaume Deraedt, *la traçabilité liée à l'authentification permet en cas de problème de trouver le responsable et évite de mettre en cause tout le service*. » Le récent accident survenu à l'hôpital Saint-Vincent-de-Paul (une erreur de produit injectable a entraîné la mort d'un enfant de trois ans) ou les irradiés d'Épinal sont encore dans toutes les mémoires de soignants.

Sans oublier qu'à l'hôpital, la première sécurité c'est le fonctionnement normal du système de santé, comme le dit Eric Grospeiller, fonctionnaire de sécurité des systèmes d'information au ministère de la Santé. « *Le médecin doit avoir confiance dans son système informatique mais il a besoin de la disponibilité immédiate des informations qu'il contient, il y aura donc toujours un arbitrage entre la sécurité et la fluidité des informations* », rappelle le Dr Jacques Lucas, vice-président du conseil national de l'Ordre, pour qui le médecin a lui aussi l'obligation de veiller à la sécurité et pourrait voir sa responsabilité engagée s'il n'en respectait pas le bon usage.

> *MARIE-FRANÇOISE DE PANGE*

Le Quotidien du Médecin du : 03/11/2009