Construire une stratégie industrielle pour sécuriser et rendre viable l'écosystème numérique de nos hôpitaux

Le 4 mars 2021

Connues de longue date des spécialistes, les attaques informatiques sur les hôpitaux deviennent si nombreuses qu'elles font tous les jours la une de nos journaux.
Alors que la situation s'aggrave et que nos hôpitaux apparaissent comme des cibles « faciles » pour les hackers et les délinquants des « ransomwares. », qui convoitent de plus en plus nos données de santé considérées à forte valeur ajoutée, il est urgent de se poser les bonnes questions.

Tout d'abord, il convient de récuser la charge gouvernementale qui revient à dire que la cause principale des attaques informatiques incombe au comportement des salariés, infirmières, médecins, qui ne « respecteraient pas les règles élémentaires de la cyber-hygiène ».
C'est oublier, par exemple, que le Président de la République, le premier, a décidé de confier à Microsoft, l'expérimentation de la mise en place de la plateforme informatique des données de santé (Health Data Hub).
La Cour de justice de l'Union européenne, la CNIL, le Conseil d'État et la CNAM récusent le projet au motif que confier l'hébergement de nos données à une société soumise au droit américain et aux programmes de surveillance permis par ce dernier n'est pas compatible avec la protection des données régie par le RGPD.
Le gouvernement, lui-même, a reconnu ce danger mais cela ne l'a pas empêché de poursuivre sans tenir compte de ces recommandations : dans le cadre de la campagne de vaccination, l'Élysée et son gouvernement ont conclu un partenariat avec Doctolib qui confie ces données à une autre société américaine Amazon Web Services. On peut mieux faire en termes de sécurité !
Au lieu de mettre une pression « morale » sur les hôpitaux, le gouvernement devrait commencer par allouer les moyens suffisants et les postes en conséquence pour que les personnels aient le temps de faire leur travail sereinement. Cela aurait un impact direct sur l'amélioration de la sûreté et de la cybersécurité de notre système de Santé. Voilà ce qui serait la base d'une bonne stratégie.

Si on en revient au système informatique hospitalier en lui-même, le problème de la sécurité dans nos hôpitaux peut s'analyser à trois niveaux.

1°) Le niveau du Matériel (Hardware), généralement le grand oublié de l'ensemble des analyses.
La plupart du temps, les architectes informatiques considèrent que toutes les ressources matérielles présentes sur le Marché (composants électroniques) se valent pratiquement en termes de fiabilité et de sécurité.
Or, la réalité est tout autre ! En effet, tout expert en cybersécurité sait qu'il est impossible de vérifier la fonctionnalité et l'intégrité d'un composant sauf à le produire soi-même. Déjà en 2011, une étude de la Cour des comptes des États-Unis démontrait que 40% des composants des systèmes de sécurité étaient contrefaits ou comportaient des portes dérobées, les « backdoors » dénoncées par Édouard SNOWDEN en 2014.
En France, les référents en cybersécurité, comme l'Agence Nationale de la Sécurité des Systèmes d'Information, interdisent d'utiliser certains processeurs car ils sont soupçonnés de transmettre des informations à la NSA …

2°) Le niveau des logiciels (Software).
En France, le choix de solutions clef en main conduit le plus souvent à l'utilisation des produits proposés par les GAFAM ou par l'industrie chinoise. Certes, certains logiciels très spécialisés sont Français (Dassault Systems) ou Européen (SAP) mais leur spécificité et leur coût les rendent inaccessibles à des applications plus larges.

3°) Le niveau de la production et de la circulation des informations dans et autour de l'hôpital.
On aborde là, la question centrale de **l'Architecture des systèmes d'informations de Santé**.
Sur ce sujet, il faut s'appuyer sur les revendications des professionnels de santé pour leur permettre de faire pleinement le métier pour lequel ils se sont formés, et pour lequel ils sont motivés.
Ces besoins qui rejoignent l'intérêt des patients s'articulent autour de trois objectifs :
- Disposer d'une informatique d'assistance et non de contrainte orchestrée par les règles de gestion de la T2A ;
- Utiliser un outil ergonomique permettant de réunir les informations et d'avoir un accès simple rapide et ubiquitaire aux données concernant le **patient** afin d'assurer une prise en charge optimale ;
- Autoriser une collecte de données anonymisées permettant la réalisation d'**études** cliniques, épidémiologiques et autres sous le contrôle des professionnels et en accord avec les patients.

Des industriels comme Dassault Systems ou Thales, mais aussi des PME et des start-up spécialisées, pourraient tout à fait mobiliser leur savoir-faire autour du Cloud, des moyens de simulation et de gestion des opérations complexes entre systèmes différents, pour construire un tel projet.
Celui-ci ne peut avancer dans la bonne direction qu'en coopération avec les parties prenantes : les intervenants de l'hôpital et les fabricants de matériels. Et cela, dès le stade de conception pour éviter en particulier les failles de sécurité.
La CGT propose de travailler ces questions au sein des Comités Stratégiques de Filière (CSF) du Conseil National de l'Industrie (CNI), le CSF industrie et technologie de la Santé, le CSF Électronique et le CSF Sécurité.

Il faut, sur le fond, repenser l'informatisation du système sanitaire.

Il faut sortir de l'approche stéréotypée des informaticiens pour qui le système d'information doit viser le recueil du maximum de données à croiser au gré des besoins des structures et des financiers.
Il faut également sortir d'une vision libérale qui conduit à sacrifier les services informatiques internes au profit de cabinets de consulting externes porteurs de solutions clef en main : on sait qu'ils visent toujours à plus de standardisation propriétaire ce qui rend le système de santé captif aux GAFA et pousse à la suppression d'emplois supports.
Une architecture bien construite doit permettre de s'affranchir largement des problèmes de comportement humain, les urgentistes ou le personnel de réanimation ne pouvant se permettre de vérifier l'authenticité d'une requête externe.

Les soignants, les directions, les structures sanitaires du territoire, n'ont pas besoin des mêmes données.

Concevoir, avec le personnel des outils adaptés répondant aux 3 objectifs relevés plus haut, permettrait une meilleure efficacité mais aussi de réduire considérablement les risques de piratage. A cela, on oppose le besoin d'interopérabilité entre les systèmes d'informations.
Cet argument fallacieux est souvent avancé pour justifier les restructurations des services et systèmes informatiques.
Il sert surtout aux marchands de matériels à rendre captif le système de santé. **En fait, il est possible de fabriquer du sur-mesure et de l'interopérable.**

> Christophe Prudhomme, porte-parole de l'Association des médecins urgentistes de France (Amuf) :
> *En ce qui concerne l'interopérabilité, je voudrais citer un exemple en rapport avec mon activité quotidienne. Premièrement, l'absence d'interopérabilité des systèmes de gestion des interventions entre les SAMU de Paris et de la petite couronne et la Brigade des sapeurs-pompiers de Paris. La conséquence est une perte de chance pour le patient lors des interventions où le facteur temps est déterminant, comme l'arrêt cardiaque. En effet, aujourd'hui que l'appel tombe sur le 15 ou le 18, la prise d'adresse se fait d'abord dans un système puis l'opérateur prend son téléphone pour contacter son collègue pour lui transmettre les informations afin qu'elles soient rentrées dans un autre système ! Deuxième carence ; l'absence d'accès direct aux dossiers de patients complexes lors d'un appel en urgence, notamment pour les patients en hospitalisation à domicile ou atteints de pathologies complexes.*

La non-centralisation, un outil de sécurité

On peut s'inspirer de l'exemple du militaire : la compatibilité entre les systèmes des diverses armées sur le champ de bataille est réalisée grâce à une normalisation de la forme des données type open source. Ceci permet l'interopérabilité tout en permettant à tout un chacun de construire du matériel sécurisé.
Cette approche permettrait aux utilisateurs qui peuvent être à l'hôpital ou en ville ou en opération (urgentistes) de partager les informations tout en n'étant pas tributaire de solutions logicielles et matérielles propriétaires. Elle permet également la décentralisation du stockage des données en réduisant la portée d'une faille de sécurité éventuelle.
Par exemple, Thales sait, sur les champs de bataille (qui ne manquent pas hélas aujourd'hui), rendre compatible et fluide toute la chaîne de détection et de commandement composée d'une multitude d'appareils et logiciels, au départ incompatibles (17 armées dans la coalition en Afghanistan).
Ici, « le handicap » renforce la protection à toute intrusion malveillante. Pourquoi, ce qui est faisable sur un champ d'opération militaire ne serait pas possible à l'échelle d'un hôpital, de nos territoires, à l'échelle de notre système de santé ?

Conclusion :

- Le développement d'une filière industrielle des dispositifs de santé comporte un volet numérique essentiel et vital pour l'amélioration des diagnostics et des soins, attendue autant par la communauté des soignants que par les patients.
- Il faut permettre au personnel de santé de s'approprier des solutions locales adaptées à la diversité de leurs besoins, la standardisation systémique n'étant pas obligatoirement la solution.
- Il faut maintenir et développer les départements Système d'Infirmations internes aux hôpitaux.
- Assurer la sécurité de tous les systèmes d'imagerie, de traitement et de stockage des données et leur interconnexion représente un enjeu considérable qui passe par une meilleure maîtrise des composants électroniques nationalement contrôlés.
- La sécurisation des bases de données générées, locales ou centralisées comme le Système National des Données de Santé (SNDS) doit être garantie par un dispositif souverain et de confiance loin de l'appétit des GAFAM, de la CIA ou autre service de surveillance.
- L'interopérabilité doit être garantie par la normalisation open source de la forme et de la génération des données.

Grégory LEWANDOWSKI coordinateur CGT Thales
Franck PERRIN Représentant CGT au CSF Industrie et Technologie de la Santé
Sylvain Delaitre Représentant CGT au CSF sécurité
Fabrice Lallement Représentant CGT au CSF Electronique