Construire une stratégie industrielle pour l'écosystème numérique de nos hôpitaux

Le 4 mars 2021

Connues de longue date des spécialistes, les attaques informatiques sur les hôpitaux font aujourd'hui la une de nos journaux. Selon les chiffres officiels, les hôpitaux français ont essuyé 27 attaques en 2020. Et depuis le début de l'année, un hôpital français est la cible chaque semaine d'une cyber-attaque, selon le secrétaire d'État chargé de la Transition numérique Cédric O.

Nos hôpitaux apparaissent comme des cibles « faciles » pour les hackers et les délinquants en rançongiciels. Ils convoitent nos données de santé, considérées à forte valeur ajoutée.

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 ».
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 !

Le problème de la sécurité dans nos hôpitaux s'analyse à trois niveaux.

1°) Le Matériel (Hardware), généralement grand oublié
La plupart du temps, les architectes informatiques considèrent que les ressources matérielles présentes sur le Marché (composants électroniques) se valent pratiquement en termes de fiabilité et de sécurité.
Or, 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, soupçonnés de transmettre des informations à la NSA .

2°) Les 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. Certains logiciels spécialisés sont Français (Dassault Systems) ou Européen (SAP) mais leur spécificité et leur coût les rendent inaccessibles à des applications plus larges.

3°) La production et la circulation des informations dans et autour de l'hôpital

C'est la question centrale de **l'Architecture des systèmes d'informations de Santé**.
Rappelons tout d'abord les revendications des professionnels de santé qui veulent pouvoir exercer pleinement leur métier.

Ce besoin qui rejoint l'intérêt des patients, s'articule autour de trois objectifs :

- Disposer d'une informatique d'assistance et non de contrainte orchestrée par les règles de gestion de la T2A[1] ;

- Utiliser un outil ergonomique permettant de réunir les informations et d'accéder simplement et rapidement, à tout moment, 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.

Sur le fond, il est nécessaire de repenser l'informatisation du système sanitaire. Et 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.

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.

Les soignants, les directions, les structures sanitaires du territoire, n'ont pas besoin des mêmes données. Concevoir, avec le personnel, des outils

[1] Tarification à l'activité : l'activité médicale définit le niveau de rémunération de l'établissement (public comme privé) entrainant une course à la rentabilité.

adaptés et autonomes, permettrait une meilleure efficacité mais aussi de réduire considérablement les risques de piratage du fait de leurs « compartimentations ».
À cela, on oppose le besoin d'interopérabilité entre les systèmes d'informations, souvent avancé pour justifier les restructurations des services et systèmes informatiques… qui œuvrent principalement au bénéfice des marchands de matériels, afin de rendre captif le système de santé.

Il est pourtant possible de fabriquer du sur-mesure et de l'interopérable.

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 sans être 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, 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 Électronique