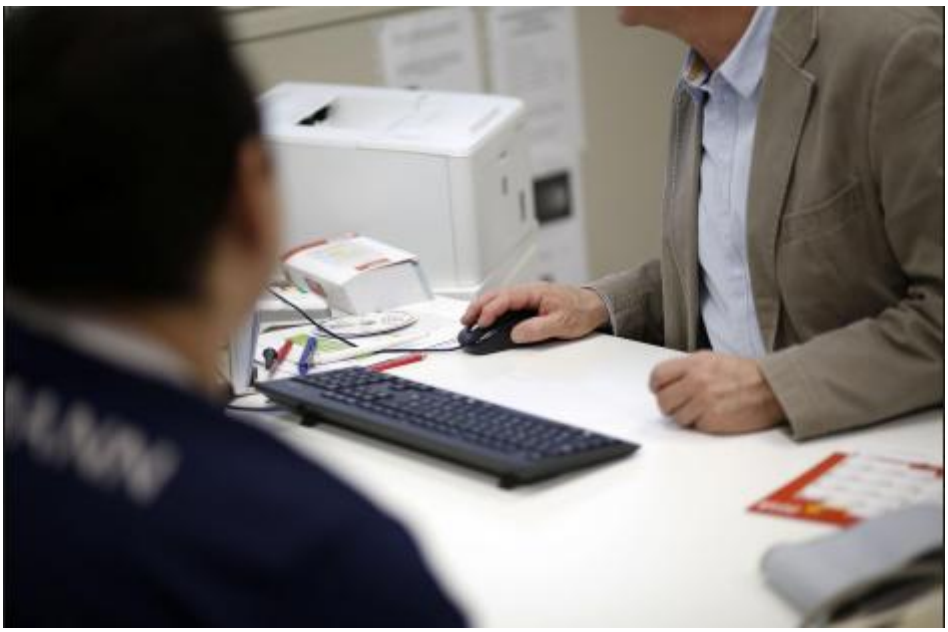
LE QUOTIDIEN DU MEDECIN.fr

Attaques informatiques, piratage, vols

Données de santé : toutes aux abris !

Sophie Martos | 28.03.2019

Sécuriser les données de santé constitue un vrai enjeu dans le monde médical. Malgré un début de prise de conscience, le manque d'investissement et de sensibilisation dans les établissements de santé et auprès des professionnels font courir un risque accru d'incidents, qui inquiète les patients.



Un mot de passe peu solide suffit aux cyberpirates pour agir
Crédit Photo : SEBASTIEN

Que ce soit en médecine de ville par les logiciels métiers ou à l'hôpital par l'informatisation et les équipements médicaux, les données de santé sont partout.

La multiplication des sources et des formats posent des questions centrales en termes d'usages, d'accès et surtout de sécurité. « Plus il y en a, plus on augmente la vulnérabilité informatique » et de facto les risques, résume Vincent Trély, fondateur et président de l'Association pour la sécurité des systèmes d'information santé (APSSIS, qui regroupe depuis 2010 des experts du secteur).

Depuis 2012, des protocoles de sécurité sont mis en place par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), notamment auprès des établissements de santé. En 2018, l'arrivée du règlement générale sur la protection des données (RGPD) est venue compléter le niveau de sécurité. Si la politique du numérique va dans le bon sens, réussir le défi de la sécurisation des données de santé est une autre paire de manches. « Cela implique des coûts financiers et des moyens humains supplémentaires », pour gérer les nouvelles tâches telles que l'exploitation de nouveaux logiciels, explique Vincent Trély. Or les établissements n'investissent pas assez. Il consacre entre 1 à 2 % de leur budget dans le numérique contre 4 à 6 % au Canada, dans les pays scandinaves ou en Suisse ».

Si l'État investit dans la transformation numérique et le développement des systèmes d'information depuis plusieurs années (400 millions d'euros dans le plan Hôpital numérique 2012-2017, puis 420 millions d'euros dans le programme HOP'EN 2018-2022), les hôpitaux ne se saisissent pas forcément de cette manne, au regard des contreparties réclamées.
« Les établissements doivent prouver qu'ils utilisent une charte de sécurité et répondre à un tas de critères pour se voir allouer une somme d'argent », poursuit Vincent Trély.

Le dossier médical à 150 dollars sur le darknet

Ce manque d'investissement dans la cybersécurité peut avoir de lourdes conséquences, en France comme ailleurs. Les exemples ne manquent pas. Le NHS, système de santé public anglais, en sait quelque chose. Ses systèmes ont été infectés par un programme malveillant de la famille des rançongiciels (appelé WannaCry) en 2017 causant le report ou l'annulation d'interventions médicales. Aux États-Unis, 176 millions de dossiers de santé ont été piratés entre 2010 à 2017. Dans l'Hexagone, le ministère de la Santé a recensé 1 341 déclarations d'attaques subies (hôpitaux, cabinets de ville, EHPAD, etc.) en 2016.

Différents types de failles sont identifiés de longue date : des mots de passe peu solides, une messagerie non homologuée, le partage d'ordinateurs, des brèches dans les logiciels ou encore dans les équipements biomédicaux. « Ces appareils exigent des connectivités au réseau des établissements. Ils ne sont pas toujours conformes aux normes de sécurité de l'hôpital et peuvent être des points d'entrée d'attaques informatiques », cite à titre d'exemple Loïc Guézo, expert cybersécurité chez Trend Micro, société qui a développé un kit complet permettant de faire un contrôle de l'état sanitaire informatique des équipements biomédicaux.

Les experts sont formels : établissements et médecins doivent prendre conscience de la nécessité de s'armer contre les cyberattaques, car les données de santé sont extrêmement convoitées : « Elles ont une grande valeur marchande, précise Vincent Trély. Sur le darknet, un dossier médical se vend entre 35 et 150 dollars. Ce que veulent les acheteurs, c'est se procurer ces données en masse cela peut se chiffrer en millions ».

Leur vol, puis leur exploitation, peut donc rapporter gros. Il est possible de faire « du chantage aux données », menacer de les dévoiler et demander une somme d'argent en échange. Des personnes malhonnêtes peuvent également monter des arnaques téléphoniques après avoir subtilisé des données personnelles sur les sites de prise de rendez-vous en ligne.

Sensibiliser tout le monde

Une partie de ces risques pourraient être endigués grâce à des formations tournées sur les bonnes pratiques. Les mauvais réflexes sont encore présents. « Les professionnels de santé utilisent des outils non homologués en santé. Ils envoient des photos ou des comptes rendus sur Snapchat, Dropbox ou par SMS », regrette Vincent Trély. L'utilisation par un praticien exerçant dans plusieurs établissements de son ordinateur portable personnel peut également générer des risques. La pédagogie est donc de mise.

Enfin, il est toujours bon de rappeler qu'en cas de non-respect de la réglementation en vigueur, les professionnels de santé et les établissements s'exposent à des sanctions de la Commission nationale de l'informatique et des libertés (CNIL) et peuvent faire l'objet de procédures juridiques menées par des patients. Chez France Assos Santé, le sujet est primordial. Les patients réclament une meilleure information sur l'utilisation et les risques associés à leurs données. « Il y a un vrai risque de mésusage, insiste Alexis Vervialle, spécialiste du sujet de l'association. Les masses de données peuvent être collectées par des acteurs privés sans que le patient n'ait son mot à dire. Les usagers ne mesurent pas encore tous les dangers que la transformation numérique peut représenter pour eux. »

Source : Le Quotidien du médecin n°9736

- Masquer