DOSSIER

Données personnelles
La sécurité numérique à marche forcée

Voilà déjà plusieurs années que la transformation numérique est en marche au sein des établissements de santé, sociaux ou médico-sociaux. Les systèmes d'information sont aujourd'hui des outils de partage et d'échanges incontournables au bénéfice des professionnels et des usagers. Revers de la médaille : ils font aussi l'objet d'attaques dont les conséquences, parfois très importantes, sont sous-estimées par les acteurs sociaux. Dans un monde de plus en plus connecté, leur sécurisation est devenue une priorité afin de conserver la confiance des usagers. Le Règlement général sur la protection des données qui doit entrer en vigueur le 25 mai 2018, devrait inciter les derniers retardataires à se préoccuper de ces enjeux. Il ne s'agit pas que d'une question de procédure mais bien de culture de la sécurité à acquérir.

Par Solenne Durox

© NORA CAROL PHOTOGRAPHY/GETTYIMAGES

L'affaire a fait la une des journaux. En mai 2017, une attaque d'une ampleur inédite touchait le service national de santé britannique (NHS). Une dizaine d'hôpitaux affirmaient avoir été infectés par un virus du type « rançongiciel » baptisé « WannaCry » avec pour conséquence immédiate la paralysie complète des réseaux téléphoniques, des services d'imagerie à rayons X et des systèmes de gestion administrative des patients. En janvier 2018, la presse révèle le vol des données médicales de plus de la moitié de la population norvégienne. Un mois plus tôt, c'était une maison de retraite suisse qui versait une rançon à des pirates pour récupérer les dossiers de ses résidents.

Dysfonctionnement potentiellement tragique

Qu'elles soient massives ou localisées, les cyberattaques se multiplient à travers le monde et n'épargnent personne. Le secteur sanitaire, social et médico-social en fait régulièrement les frais. Si l'utilisation des nouvelles technologies améliore indéniablement la communication, la gestion et la sauvegarde des données ou la qualité des soins, elle est aussi porteuse de risques et de contraintes qui vont en s'accroissant de manière exponentielle. Il y a quinze ans, le principal enjeu de la sécurité des systèmes d'information (SI) était d'avoir un antivirus à jour, au cas où… Aujourd'hui, la dépendance des soins au numérique et le développement des objets connectés, rendent toute panne ou dysfonctionnement potentiellement tragique. Actes malveillants, sinistres naturels ou simples erreurs de maintenance…, le panel des menaces est large et impacte la confidentialité, la disponibilité ou l'intégrité des données. On a souvent tendance à se focaliser sur la première alors que les deux autres sont tout autant, voire plus, préjudiciables dans le domaine de la santé notamment. La fuite de dossiers patients n'a jamais tué personne alors qu'une erreur de prescription de médicaments en pédiatrie à cause d'un logiciel défaillant peut s'avérer désastreuse.

Pas assez d'investissement

Parmi les incidents les plus courants, on trouve les pertes ou fuites de données. « Elles sont souvent à mettre sur le compte de professionnels qui font des bêtises mais sans forcément vouloir nuire », explique Vincent Trély, président de l'Association pour la sécurité des systèmes d'information de santé (APSSIS). Ils vont par exemple ouvrir des plateformes de partage Dropbox ou Google drive et y partager des données de santé entre plusieurs hôpitaux ». Le tout finira immanquablement par se retrouver sur internet. Il y a ensuite ce qu'on appelle la cybercriminalité, souvent des escroqueries pas très compliquées qui consistent à voler ou verrouiller les données en demandant de l'argent en échange. Vincent Trély donne l'exemple de coups de fil passés par un robot à des patients. « Ils leur demandent de mettre à jour leurs dossiers médicaux en appuyant sur des boutons sur leur téléphone ce qui entraîne une

80 %
des Français
estiment que l'e-santé permet d'améliorer la coordination des professionnels de santé.

DOSSIER MÉDICAL
Les Français sont prêts à rendre accessibles leurs données de santé personnelles :

à leur médecin (90 %) | à leur pharmacien (68 %) | à leur opticien (51 %) | à leur mutuelle (47 %) | à leur assureur (17 %)

Source : étude santé Deloitte 2017.

surtaxe ». L'inventivité de ces cybercriminels et leur capacité à se renouveler pourraient presque forcer l'admiration si elles ne posaient pas autant de problèmes. Pourtant, face à l'ampleur de la menace, la part du budget consacrée à la sécurité des systèmes d'information reste modeste. Pour le secteur de la santé, elle s'élèverait en moyenne à 6 % en 2016 contre 16 % pour l'industrie selon une étude de Symantec. Or, ne pas investir c'est s'exposer à des dépenses parfois importantes. À titre d'exemple, une intrusion avec mise hors service des systèmes d'information d'une agence régionale de santé (ARS) pendant 24 heures a engendré des coûts d'intervention par un prestataire de l'ordre de 10 000 euros et une perte de productivité estimée à près de 40 000 euros, soit un total de 50 000 euros. Un cryptovirus en Ehpad a coûté 50 000 euros en coûts directs et indirects. Le piratage du standard d'un centre hospitalier a généré une surfacturation de téléphonie de l'ordre de 40 000 euros.

Un sujet de gouvernance

C'est un fait, les acteurs concernés par cette problématique ne sont pas au même niveau de maturité. « Les organismes de prestations sociales ont tous des équipes de sécurité à leur disposition car ils gèrent des flux financiers. Comme les banques, ils sont déjà soumis à des réglementations », affirme Philippe Loudenot, fonctionnaire de sécurité des systèmes d'information des ministères chargés des Affaires sociales. À l'opposé, le médico-social, à l'exception de certains grands groupes privés, semble être le parent pauvre de la sécurisation des systèmes d'information. Les petites maisons de retraite publiques n'ont généralement pas d'informaticien dédié. Pour éviter que la prise de conscience se fasse dans la douleur, il importe que la dynamique autour de la sécurité du SI soit impulsée par les directions elles-mêmes. « Les méthodes et outils de la sécurité numérique ne manquent pas, mais ils perdent toute efficacité s'ils ne sont pas soutenus en permanence », rappelle Cécile Courrèges, directrice générale de l'offre de soins. Nul besoin de dépenser une fortune pour renforcer significativement la sécurité. L'humain demeurant la principale faille, la sensibilisation et la formation du personnel aux bons usages peuvent pallier le manque d'outils. La création des groupements hospitaliers de territoire offre également l'opportunité de réaliser des économies en mutualisant la fonction centrale de responsable de la sécurité du système d'information (RSSI).

REPÈRES

- **« La sécurité du système d'information des établissements de santé »,** 2e édition, de Cédric Cartau, Presses de l'EHESP.
- **« Mémento à l'usage du directeur d'établissement de santé »,** édition 2017 de la Direction générale de l'offre de soins (DGOS) à télécharger sur solidarites-sante.gouv.fr
- **« Guide de bonnes pratiques »** sur cyberveille-sante.gouv.fr
- **Circulaire du 4 juillet 2017** relative aux mesures de sécurisation dans les établissements et services sociaux et médico-sociaux.
- **« Guide d'hygiène informatique »** de l'ANSSI sur ssi.gouv.fr

Obligation de signaler les incidents

Les structures qui ont pris du retard n'auront bientôt pas d'autre choix que de se convertir à marche forcée. Le cadre législatif et réglementaire s'étoffe et devient de plus en plus contraignant. Depuis le 1er octobre 2017, les établissements de santé, laboratoires de biologie médicale, hôpitaux des armées et centres de radiothérapie ont l'obligation de déclarer leurs incidents de sécurité informatique via le portail dédié de signalement des événements sanitaires indésirables. « Tous ces signaux forts ou faibles nous permettent de générer des alertes à l'ensemble des acteurs », observe Philippe Loudenot. Parallèlement, le ministère des Solidarités et de la Santé a mis en place la cellule accompagnement cybersécurité des structures de santé (cellule ACSS) afin d'apporter un appui aux organismes concernés par la déclaration de ces incidents. Les établissements doivent aussi se référer à la politique générale de sécurité des systèmes d'information en santé (PGSSI-S), à la politique de sécurité des systèmes d'information pour les ministères chargés des Affaires sociales (PSSI MCAS), et au référentiel général de sécurité (RGS). Sans oublier les décrets confidentialité et hébergeur entre autres. Un foisonnement de textes dans lesquels il n'est pas toujours simple de se retrouver.

Le RGPD responsabilise les acteurs

Le niveau des exigences va encore sensiblement s'élever avec l'entrée en vigueur le 25 mai 2018 du RGPD qui entraîne une refonte de la loi Informatique et libertés, en vigueur depuis 1978. Le règlement européen va renforcer les droits des personnes et la sécurité des données personnelles. Si de nombreuses formalités auprès de la Cnil disparaissent, en contrepartie, le RGPD responsabilise l'ensemble des acteurs, sous-traitants y compris. « Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité », explique la Cnil sur son site. Parmi les obligations majeures, la tenue d'un registre interne, l'analyse d'impact, la notification des violations et la nomination d'un délégué à la protection des données (DPO ou DPD). En cas de non-respect, des sanctions extrêmement dissuasives sont prévues : jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires. De quoi faire réfléchir… ◆

SANTÉ

Une charte pour les e-rendez-vous médicaux

L'URPS Médecins libéraux Ile-de-France a fait signer une charte de confiance aux plateformes de rendez-vous en ligne afin de protéger les utilisateurs.

Prendre un rendez-vous en ligne avec son médecin est aujourd'hui aussi simple que de réserver une chambre d'hôtel sur internet. Pour le patient, les avantages sont nombreux. Internet permet d'accéder en autonomie à l'agenda de son médecin à tout moment de la journée ou de la nuit. Du côté des médecins, la plateforme facilite la gestion du planning et permet de désengorger le standard téléphonique.

Déontologie médicale

Ces bénéfices ne doivent pourtant pas occulter les risques liés au développement de ce genre de services lancés par des éditeurs qui ne relèvent pas du code de la santé publique. C'est pourquoi l'URPS Médecins libéraux Ile-de-France a élaboré et publié en février dernier une charte pour la protection des utilisateurs des plateformes de prise de rendez-vous médicaux en ligne. Dix d'entre elles l'ont d'ores et déjà signée. Deux autres devraient suivre. Toutes s'engagent à appliquer les principes de respect de la déontologie médicale, de confidentialité et du secret médical. Le document comporte également des exigences fondamentales de sécurité et de fiabilité en matière de protection des données de santé collectées par ces services en ligne.

Les plateformes s'engagent notamment à respecter la réglementation sur la protection des données à caractère personnel résultant de la loi Informatique et libertés et du RGPD. Les mesures mises en place par les outils de e-rendez-vous « doivent notamment conduire à la minimisation des collectes et traitements de données, à la limitation des durées de conservation, à la sécurisation, et à l'interdiction de toute autre éventuelle utilisation ultérieure des données à caractère personnel. Une information transparente doit être apportée au médecin et au patient pour les informer des traitements des données réalisés de même que doit être recueilli le consentement préalable des utilisateurs à l'occasion de toute éventuelle utilisation de données y compris à des fins d'études et de statistiques sur les pratiques des médecins utilisateurs », détaille la charte.

REPÈRES

- **Fin 2016, plus de 20 000 médecins en France** utilisaient les services d'une plateforme de rendez-vous en ligne selon les éditeurs.
- **Le 15 février 2018, la charte a été signée par 10 plateformes :** Alaxione, Allodocteur, Calendovia, DocAvenue, Doctolib, Docteur rendez-vous, Keldoc, LogicRDV, MadeforMed, Mondocteur.fr
- **Contact :** URPS Médecins libéraux en Ile-de-France, 01 40 64 14 70, secretariat@urps-med-idf.org

Projet de certification

La plateforme doit par ailleurs recourir à des prestataires hébergeurs de données de santé exerçant une activité autorisée. L'élaboration de la charte a nécessité beaucoup de discussions avec les plateformes. « Le plus problématique concernait l'exploitation des data. Doctolib, notamment, considérait que le motif de consultation n'était pas une donnée de santé. La mise en conformité avec le RGPD nous a fourni les arguments nécessaires pour tous les convaincre », explique le docteur Laurent de Bastard, coprésident de la commission pratiques libérales et nouvelles technologies de l'URPS Ile-de-France. Un bilan d'application de la charte sera réalisé d'ici à un an et pourrait aboutir à un projet plus concret de certification. ◆

Docteur Laurent de Bastard, coprésident de la commission pratiques libérales et nouvelles technologies URPS Ile-de-France

DR

« Certaines solutions n'offraient pas toutes les précautions »

« Depuis deux ans, l'URPS étudie comment les nouvelles technologies font évoluer nos modes d'exercices en tant que médecins libéraux. L'un des premiers travaux que nous avons menés est une étude de marché sur les plateformes de rendez-vous en ligne fin 2016. Certains médecins y voyaient un moyen de faciliter l'accès aux soins tandis que d'autres craignaient de perdre la main sur leur patientèle tout en encourageant un certain consumérisme. Nous avions eu aussi des retours négatifs de confrères qui, après avoir voulu changer de plateforme, n'avaient pas pu récupérer tous leurs fichiers patients. Des questions se posaient aussi quant à l'actionnariat, certaines sociétés d'assurance ayant investi dans ces outils de prise de rendez-vous en ligne. Notre étude a abouti à un comparatif d'une quinzaine de solutions sur un marché qui en compte une cinquantaine. L'analyse de l'offre nous a permis de constater que certaines solutions n'offraient pas toutes les précautions en matière de sécurité et protection des données, notamment un hébergement agréé des données de santé à caractère personnel. C'est de là qu'est née l'idée de la charte. »

SOCIAL

La Cnaf anticipe sa mise en conformité avec le RGPD

La branche famille de la sécurité sociale gère les données de 60 millions de personnes. Pour renforcer leur protection, elle a démarré très tôt son projet de mise en conformité avec le règlement général sur la protection des données.

Voilà déjà six ans que le sujet est au cœur des réflexions. « Dès qu'on a su qu'il y aurait une évolution de la réglementation européenne, nous nous sommes mis en veille par le biais de la Cnil, du G29 (Groupe de travail Article 29 sur la protection des données). Nous avons aussi eu des échanges utiles au sein de l'Association française des correspondants aux données personnelles (AFCDP) », explique Marie-Noëlle Séhabiague, directrice de la mission analyse de la conformité informatique et libertés et de la sécurité du système d'information de la Caisse nationale des affaires familiales (Cnaf).

Centre d'opérations de sécurité

Cette mobilisation est à la hauteur des enjeux pour la branche famille de la sécurité sociale. Cette dernière gère en effet les données particulièrement sensibles de 60 millions de personnes, aussi bien ce qui concerne leur identification, leur situation professionnelle ou familiale, leurs revenus et leurs coordonnées bancaires. « Nous avons également dans nos bases tout ce qui relève de la gestion du logement, la situation sociale, voire les difficultés des personnes liées au handicap par exemple », ajoute Marie-Noëlle Séhabiague. Depuis trois ans, toutes ces données sont conservées en double dans deux datas centers situés dans deux villes en France de manière à garantir leur intégrité. La Cnaf dispose également d'un centre d'opérations de sécurité (SOC) chargé de surveiller le fonctionnement du réseau et de prendre en charge les incidents. Comme toute grande entreprise, la Cnaf est constamment l'objet de cyberattaques externes. « Nous comptons en moyenne 3 000 requêtes malicieuses par mois. Malgré les moyens de protection, le nombre d'attaques par messagerie reste élevé », indique Marie-Noëlle Séhabiague.

Afin de se mettre en conformité avec le RGPD, un plan d'action a été mis en œuvre. Certaines ont déjà été réalisées, d'autres le seront d'ici au 25 mai 2018 ou au-delà. « La conformité est un travail de longue haleine, un marathon sans fin ». En termes de gestion des risques, la Cnaf s'est lancée dans un chantier d'anonymisation des données. Elle a revu l'année dernière l'intégralité de sa politique liée à la sécurité du SI. Les chartes nationales d'utilisateur et d'administrateur ont complètement été remises à plat et présentées au sein des différents services et caisses. Des rappels réguliers sont aussi faits en ce qui concerne le secret professionnel.

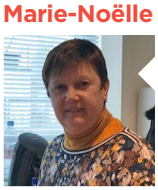
REPÈRES

- **Caf.fr** est le premier site consulté dans la catégorie sécurité sociale.
- **Le CIL** est mutualisé pour la quasi-totalité des 102 caisses locales. Pour les 18 caisses qui ont désigné leurs propres CIL, ces derniers seront maintenus jusqu'au 25 mai 2018.

Procédures internes

Autre point important : la mise en place de procédures internes afin de notifier dans les meilleurs délais toute violation de données comme le prévoit le règlement. Ce sera fait systématiquement en direction de la Cnil et au cas par cas pour les usagers. Pour ces derniers, le responsable de traitement prendra sa décision en fonction du volume et de la nature des données. « Si elles sont chiffrées, le risque pour la vie privée est moindre par exemple », remarque Marie-Noëlle Séhabiague pour qui le plus gros des défis reste la documentation exhaustive et permanente des actions réalisées. ◆

Marie-Noëlle Séhabiague, directrice de la mission analyse de la conformité informatique et libertés et de la sécurité du SI



DR

« Le DPO sera mutualisé »

« À la Cnaf, le correspondant informatique et libertés (CIL) ne se limite pas à une seule personne. Je suis secondée par trois chefs de projet informatique et liberté, un chef de projet sécurité informatique et une attachée de direction. Le CIL est mutualisé pour la quasi-totalité des caisses et ce sera aussi le cas du délégué à la protection des données (DPO) quand il sera nommé. C'est un choix que nous avons fait dès 2013. À l'époque, nous accusions un certain retard par rapport aux autres branches du régime général qui avaient toutes désigné des CIL dans chaque caisse. Ce retard s'est transformé en une opportunité avec le RGPD. Cette mutualisation effective en 2017 s'est imposée pour plusieurs raisons. Cela permet de concentrer les connaissances et expertises, d'avoir une application homogène de la doctrine sur l'ensemble du territoire ainsi qu'une visibilité de l'état de la conformité et des demandes qui peuvent être formulées par les usagers. »

POINTS DE VUE

Les professionnels de santé sont-ils prêts pour la cybersécurité ?

Pour Vincent Trély, convertir les établissements et le personnel à la sécurité numérique est un travail de longue haleine qui passe par la sensibilisation et le compromis. Cédric Cartau plaide pour que le sujet soit désormais considéré d'un point de vue stratégique et plus seulement technique. Et vu comme un vecteur de performance.

Une importante cyberattaque contre les établissements de santé et médico-sociaux français comparable à celle vécue par le National Health Service (NHS) est-elle inéluctable ?

Vincent Trély : L'attaque de WannaCry contre le système de santé anglais n'était pas ciblée, elle était mondiale. Le NHS en a été victime à cause d'un certain nombre de failles, notamment parce que ses vieux systèmes d'information n'étaient pas à jour. En France, le parc informatique évolue plus régulièrement heureusement. Par ailleurs, nos établissements de santé ne sont pas interconnectés comme en Angleterre. Donc ils ne sont pas tous exposés en même temps et de la même manière. Il n'en reste pas moins que la France fait partie de la quinzaine de pays dans le monde dont la santé est informatisée. Nos établissements peuvent donc être visés. Avec au moins un million de nouveaux virus par jour, le risque est certain, qu'on soit un grand hôpital ou un petit Ehpad. D'autant plus que les données de santé ont de la valeur. À titre d'exemple, le prix d'un dossier médical piraté s'élève entre 30 et 200 dollars. Il y en a plusieurs millions à vendre actuellement sur le darknet. Leur cote évolue, un peu comme à la Bourse. Ce qui motive les acheteurs ce n'est pas un dossier médical en particulier mais d'en avoir un très grand nombre, le but étant de constituer une importante base afin d'en tirer des tendances.

Cédric Cartau : Nous sommes loin d'être mauvais en matière de cybersécurité en France même si d'autres pays sont beaucoup plus acculturés à la notion de risque. Cependant, la santé accuse un net retard en comparaison d'autres secteurs comme la banque ou l'industrie. Généralement, en France, tant qu'il n'y a pas eu de catastrophe, personne ne bouge. C'est un vrai problème. Imaginez qu'on tombe parfois sur des hôpitaux ou des Ehpad où aucun antivirus n'a été installé sur les postes de travail… J'en connais d'autres où le pare-feu date d'il y a quinze ans ! Les préconisations de base ne sont malheureusement pas appliquées dans la majorité des endroits. Citons par exemple ce très gros hôpital qui, en 2016, a perdu tous ses fichiers car il n'avait pas respecté une règle élémentaire. Il leur a fallu une semaine pour tout restaurer.

Convertir les gens aux bonnes pratiques est encore plus compliqué dans l'environnement de santé car on ne met pas les médecins au pas facilement

©APSSIS

Vincent Trély, consultant spécialisé en stratégies numériques de santé et en management des processus systèmes d'information. Il est le président de l'Association pour la sécurité des systèmes d'information de santé (APSSIS).

Pourquoi ces enjeux ne sont-ils pas pris suffisamment au sérieux ?

VT : Rappelons que le développement du numérique est relativement récent dans le monde de la santé. Avant, l'informatique ne concernait que les ressources humaines à l'hôpital pour la paie notamment. Cela ne fait que dix ou quinze ans que se sont développés les logiciels de soins, les dossiers patients informatisés, les clichés numériques de radiologie. Il y a de plus en plus de réseaux et de failles. Confronté à des difficultés économiques, le système de santé a un peu de mal à encaisser tout ça. Dans les hôpitaux, on rechigne à acheter des outils de sécurité onéreux qui ne sont pas en lien direct avec le patient. Lorsqu'un directeur des systèmes d'information demande à son directeur général d'investir 180 000 euros, il a en face de lui un médecin qui explique que cela fait deux ans qu'il attend un mammographe pour le même prix. Et c'est souvent ce dernier qui gagne.

CC : Une majorité des gens pensent que la sécurité des SI nécessite beaucoup d'argent. Or, on peut faire beaucoup de choses sans dépenser un euro. Gardons à l'esprit que si la sécurité coûte cher, la non-sécurité encore plus. On gagnerait beaucoup à considérer le problème d'un point de vue stratégique et pas seulement technique comme c'est souvent le

cas. Les décideurs confondent fréquemment informatique et systèmes d'information. Pour quelques-uns, le RSSI est la personne qui installe les PC sur les bureaux… Onze mois par an, il est invisible et inaudible. On se rend compte de sa présence et de son utilité seulement quand il y a un problème. Il n'existe qu'une cinquantaine de RSSI pour plus de 1 000 établissements publics en France. Certains n'en ont que le titre car ils sont cantonnés au paramétrage des antivirus ou à la gestion du pare-feu. Cette vision du métier est vraiment réductrice. L'aspect organisationnel est pourtant très important. En tant que RRSI du CHU de Nantes, je passe plus de temps à tester les procédures et à sensibiliser les équipes. Je suis en amont de tous les projets. Mon rôle est de faire des analyses de risques et des recommandations à ma direction générale.

Comment peut-on sensibiliser les professionnels ?

VT : On assiste à une prise de conscience depuis trois ans. La sécurité commence à devenir un sujet à part entière dans une partie des établissements. Certains hôpitaux organisent des journées de sensibilisation de tout leur personnel, métier par métier. Parfois, ce sont même les agences régionales de santé qui financent ces opérations. Cela reste insuffisant. Le problème, c'est qu'on a déployé de l'informatique sans se demander si les soignants savaient comment cela fonctionne. Ce n'est pas une population naturellement issue du numérique. Il faut souvent reprendre les bases : ne pas écrire son mot de passe sur son écran ou utiliser la messagerie sécurisée par exemple. D'une manière générale, le responsable sécurité est perçu comme quelqu'un d'assez pénible. Convertir les gens aux bonnes pratiques est encore plus compliqué dans l'environnement de santé car on ne met pas les médecins au pas facilement. Cela prend du temps. J'ai pu moi-même le constater quand j'ai été nommé DSI au CH du Mans il y a déjà plusieurs années. À l'époque, j'avais tenté d'expliquer aux urgentistes qu'ils allaient devoir utiliser une carte à puce pour accéder à leurs ordinateurs. La réunion a pris fin très rapidement. Les urgentistes m'ont dit : « vous n'avez pas compris ce que nous faisons comme boulot ici ». Quelques mois plus tard, on s'est tous à nouveau réuni autour d'une table. On a discuté et les choses se sont améliorées progressivement. Il y a un paradoxe dans le monde de la santé qu'on peut tout à fait entendre. La sécurité amène des contraintes. Or, les soignants qui sont mobiles ont besoin d'accéder à l'information tout le temps, partout et très vite. Tout l'enjeu est de trouver un juste compromis afin d'éviter les rejets. Et de s'adapter en fonction des situations et des métiers.

CC : Paradoxalement, je ne rencontre pas de problème avec le corps médical car les médecins sont acculturés à la notion de risque, notamment les biologistes qui connaissent les normes ISO 2000 depuis vingt ans. Même les urgentistes ne posent aucun souci. C'est un peu plus problématique avec la gestion technique des bâtiments dont le système n'était pas jusqu'alors géré par l'informatique. Les plus compliqués à gérer sont les fournisseurs d'appareils biomédicaux. Il faut savoir que ce matériel de pointe très onéreux que sont les IRM, mammographes, scanners et automates de laboratoire se connectent à des ordinateurs. Pourtant, ils ne sont équipés d'aucun antivirus. En cas d'attaque, on est obligé de les débrancher !

On tombe parfois sur des hôpitaux ou des Ehpad où aucun antivirus n'a été installé sur les postes de travail

©CHU RENNES

Cédric Cartau, responsable de la sécurité des systèmes d'information au CHU de Nantes et chargé de cours à l'École des hautes études en santé publique (EHESP). Il est l'auteur du livre « La sécurité du système d'information des établissements de santé ».

Le RGPD peut-il contribuer à accélérer le mouvement ?

VT : Sur ce sujet, il reste aussi de la pédagogie à faire car si 100 % des DSI et responsables de sécurité savent à quoi correspond le RGPD, ce n'est pas le cas pour la moitié des directions générales. C'est compréhensible car elles sont déjà noyées par le réglementaire. Il faut pourtant que les établissements s'en préoccupent rapidement car le RGPD va notamment les obliger à prévenir la Cnil et le patient sous 72 heures en cas de violation de données. Les incidents qui étaient jusqu'alors étouffés, ne pourront plus l'être. On risque de voir plus de cas apparaître dans la presse. Pour autant, il est inutile de paniquer. Personne ne sera en conformité le 25 mai. La Cnil sera tolérante sur certains volets comme la documentation. Toutefois, si un établissement essaie de cacher une violation de données, elle aura sans doute moins d'états d'âme. L'important pour la Cnil est de voir que le chantier est lancé. Les pénalités ne seront pas immédiatement appliquées. On voit mal par ailleurs l'État infliger une amende de 400 000 euros à un hôpital public tout en sachant que celui-ci est déjà déficitaire. ◆

VU D'AILLEURS

L'Estonie concilie e-santé et sécurité

Présenté comme l'un des leaders mondiaux en matière de cybersécurité, le pays balte l'est aussi en matière de e-santé. Et plus que tout, il réussit à concilier les deux.

En 2007, l'Estonie a été la cible de la première cyberattaque souveraine. Durant deux semaines, de nombreux sites ont été bloqués, dont ceux du Parlement, de banques, ministères, journaux et stations de télévision. En réaction, l'Estonie a mis les bouchées doubles. Seulement un an plus tard, le centre de cyberdéfense de l'Otan entrait en service à Tallinn. Le pays a également prévu d'ouvrir cette année au Luxembourg la première e-ambassade afin d'y garder ses banques de données.

Vie digitalisée

Cette mesure n'a rien d'un luxe car en E-stonie, comme on la surnomme aujourd'hui, toute la vie des habitants est digitalisée. Les démarches administratives sont dématérialisées, à l'exception des mariages, des divorces et des ventes immobilières. Les Estoniens les réalisent grâce à une « carte d'identité numérique », obligatoire dès 15 ans. On y trouve les informations personnelles et médicales, le casier judiciaire et le permis de conduire des habitants. Avec elle, ils peuvent voter en ligne même à l'autre bout du monde, payer leur abonnement de bus, et leurs impôts.

Dossier médical électronique

Comme tous les systèmes de données de l'État, celui de la santé est interconnecté depuis 2008 grâce à la plateforme de gestion X-Road. Chaque Estonien dispose d'un dossier médical électronique centralisé accessible à tous les professionnels. Les prescriptions peuvent se faire directement en ligne. Le patient n'a qu'à présenter sa carte d'identité numérique dans une pharmacie pour obtenir ses médicaments. « Quand un blessé est pris en charge par une ambulance, il n'est pas encore arrivé aux urgences que son historique s'affiche déjà sur les ordinateurs de l'hôpital grâce à ce système », explique Pierre-François Laget, ancien responsable de l'information médicale dans un important centre hospitalier régional et président de l'Atelier Estonie du forum d'ingénieurs Forum Atena.

Sanctions en cas de violation

La grande disponibilité des données va de pair avec une vraie politique de protection et confidentialité. Lorsqu'ils suivent un patient, les professionnels déposent une demande pour consulter ses données sauf si celui-ci a expressément choisi de ne pas rendre ses informations accessibles. Le personnel médical et infirmier a l'obligation éthique de s'assurer que leur démarche est bien justifiée. Les hôpitaux font d'ailleurs l'objet d'inspections régulières pour s'assurer qu'aucune violation du secret médical n'a été commise, avec menace de sanctions allant jusqu'à la révocation. Autre garde-fou : « les Estoniens peuvent aussi savoir en un clic qui a eu accès à leur dossier médical, quelles données ont été consultées, ce qui est assez dissuasif », estime Pierre-François Laget. Patients et professionnels peuvent voir les mêmes informations médicales : résumés des diagnostics, tests, détails des opérations, prescriptions numériques… Difficile de faire plus transparent. ◆

ESTONIE

- **Population :** 1,3 million d'habitants en 2016.
- **PIB par habitant :** 15 900 euros.
- **Espérance de vie :** 72,2 ans pour les hommes et 81,4 ans pour les femmes en 2015.
- **Sentiment d'être en bonne santé :** 51 %.
- **Renoncement aux consultations en raison du coût :** 9,7 % en 2016.
- **Taux de médecins en exercice :** 3,4 pour 1000 habitants en 2015.
- **Taux de la population couverte par l'assurance maladie publique :** 94 % en 2015.
- **Part des plus de 80 ans :** 5 %.

Pierre-François Laget, ancien responsable de l'information médicale dans un important centre hospitalier régional et président de l'Atelier Estonie du forum d'ingénieurs Forum Atena

DR

« Le système de santé a été construit autour du DMP et non l'inverse »

« Les données médicales sont plus en sécurité en Estonie qu'en France. Chez nous, chaque médecin a son propre système informatique, chaque hôpital, son entrepôt de données et son responsable de la sécurité informatique. En Estonie, tout est centralisé et connecté. Le système de santé a été construit autour du dossier médical partagé (DMP) et non l'inverse. En prenant son indépendance, le pays s'est débarrassé de la lourdeur administrative soviétique. Il lui restait tout à inventer, de l'état civil au réseau bancaire, en passant par son administration fiscale. Il a tout misé sur le numérique pour rattraper son retard. Ils ont compris que les autoroutes de l'information représentaient l'avenir. C'est d'ailleurs pour cela qu'aujourd'hui, en Estonie, les nouvelles technologies sont au cœur de l'éducation. Les enfants apprennent la robotique et le code informatique dès l'école élémentaire. On leur explique aussi ce qu'est la cybersécurité ou comment se servir de leur smartphone de manière intelligente. »