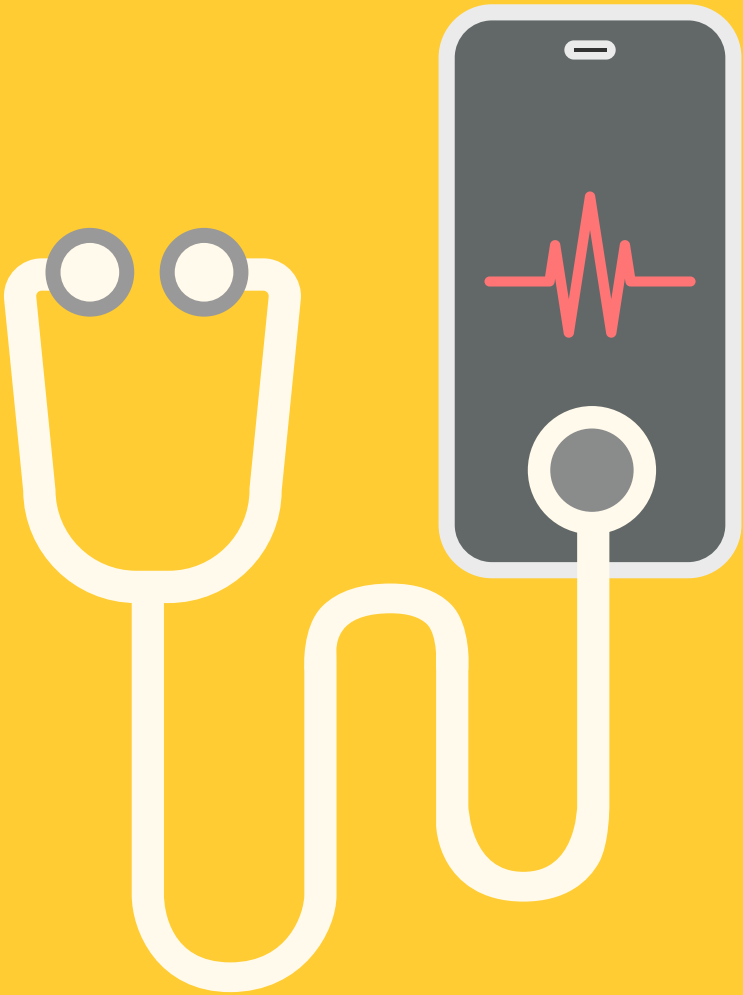


ÉCONOMIE, EMPLOI ET TRAVAIL

FÉVRIER 2020

CYBERSÉCURITÉ : ACCOMPAGNER UN SYSTÈME DE SANTÉ EN PLEINE MUTATION

RENAISSANCE numerique

TABLE DES MATIÈRES

INTRODUCTION

Le secteur de l'offre de soins[1] figure sans conteste parmi les domaines d'activité les plus exposés – et les plus à risque – aux attaques informatiques. Ces dernières années, des cyberattaques d'une ampleur sans précédent ont touché des établissements de santé, avec, parfois, des répercussions sur les activités de soins. Parmi les récents exemples figurent les « *ransomwares*[2] » qui ont visé le centre hospitalier universitaire (CHU) de Rouen en novembre 2019[3] (arrêt total de l'ensemble du système informatique entrainant des délais très longs de prise en charge, 300 000 euros de rançon demandés), ainsi que le groupe Ramsay Générale de Santé à la fin de l'été 2019[4] (120 établissements de santé en France, blocage de la messagerie et des applications métiers utilisées par le personnel). Trois mois plus tôt, c'était le CHU de Montpellier qui était la cible d'une attaque par hameçonnage[5] (649 ordinateurs

1 Voir l'infographie publiée sur le site des Agences régionales de santé intitulée « Les chiffres clés 2018 de l'offre de soins » et disponible à cette adresse : https://www.ars.sante.fr/les-chiffres-cles-2018-de-loffre-de-soins

2 Selon l'Agence nationale de sécurité des systèmes d'information (ANSSI), un rançongiciel ou *ransomware* est une technique d'attaque courante de la cybercriminalité qui consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

3 « Attaque informatique au CHU de Rouen : une enquête ouverte », *Le Monde.fr*, 18 novembre 2019.

4 « Le groupe Ramsay Générale de Santé victime d'une attaque informatique », *ZDNET*, 14 août 2019.

5 « Le CHU de Montpellier victime d'une attaque informatique : plus de 600 ordinateurs infectés », *France3.fr*, 17 mai 2019.

infectés, plus de 800 consultations fortement perturbées, impossibilité de traiter les urgences du SAMU pendant une demi-journée). Cette nouvelle vague de cyberattaques semble avoir débuté avec le virus « *WannaCry*[6] » qui défrayait la chronique en 2017 en paralysant, entre autres, seize hôpitaux britanniques.

La diffusion rapide des outils et des usages numériques au sein du système de santé, couplée aux logiques de rapprochement inter acteurs, accroissent *de facto* la surface d'exposition aux cyber risques. Les attaques sont de plus en plus importantes, sophistiquées et ciblées. Selon Guillaume Poupard, Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), leur nombre serait passé d'une tous les mois ou tous les deux mois, à une par semaine en un an seulement[7]. Les motivations des attaquants peuvent être de différentes natures selon la méthode utilisée[8], mais l'un des principaux *modus operandi* semble pour l'instant concerner le vol de dossiers médicaux de patients pour les restituer moyennant une rançon. Au-delà des cyberattaques, il existe également un « risque quotidien » auquel doivent faire face les professionnels de santé. Pour illustration, le média *ProPublica* rapportait en septembre 2019 que des données de santé de millions d'Américains se trouvaient sur la toile, en libre accès, en raison de serveurs non protégés[9]. Ce risque est particulièrement sérieux compte tenu des spécificités du système de santé, marqué par une grande interconnexion, des architectures informatiques parfois très hétérogènes - nombre d'établissements sont encore peu matures sur les enjeux de cybersécurité - ainsi que le caractère hautement sensible des données de santé[10] [11]. Depuis quelques années, le secteur de la santé est même passé en tête des domaines où les risques financiers relatifs aux failles de sécurité informatiques sont les plus importants, devant le secteur bancaire. En effet, selon une étude réalisée en 2017 par le cabinet américain *Ponemon Institute*, les coûts associés à une violation de données, rapportés à un individu, y sont près de deux fois et demi supérieurs (380 dollars) que la moyenne de tous les autres secteurs confondus (141 dollars).

Ainsi, après avoir analysé en 2018 la position spécifique en matière de cybersécurité des TPE et PME dans la chaîne de production[12], le think tank Renaissance Numérique a décidé de s'intéresser aux enjeux de cybersécurité dans le système de santé et d'interroger les capacités de résilience de ce secteur en profonde transformation numérique. Cette réflexion s'est traduite par l'organisation d'une table ronde le 25 octobre 2019 à l'occasion du mois européen de la cybersécurité, en partenariat avec Kaspersky France[13].

Elle fait aussi écho au déploiement de la stratégie nationale « Ma Santé 2022 » et à l'adoption de la loi relative à l'organisation et à la transformation du système de santé. Le volet numérique de ce texte (cf. Titre III « Développer l'ambition numérique en santé ») prévoit notamment la création d'une plateforme des données de santé, l'ouverture automatique d'un Dossier médical personnel (DMP) pour tous les bénéficiaires de l'assurance maladie, et le déploiement de la télémédecine[14]. Le texte inclut également plusieurs dispositions relatives à la collecte, au traitement, au partage et à la sécurisation des données des patients, qui seront complétées par plusieurs décrets du Conseil d'État. Cette phase de transition est une opportunité pour l'ensemble du système de santé de monter en maturité sur les enjeux de cybersécurité.

Cette note explore tour à tour les spécificités du secteur de la santé en matière de cybersécurité, ainsi que des facteurs clés pour améliorer la cyber-résilience des acteurs du parcours de soins.

6 « WannaCrypt : les hôpitaux britanniques paient leur mauvaise politique de mise à jour », *Numerama*, 16 mai 2017.

7 « Les hôpitaux français dans le collimateur des pirates informatiques », *L'Express*, 25 juin 2019.

8 Une typologie des principales attaques informatiques se trouve en introduction de la note de Renaissance Numérique « Cybersécurité : vers la responsabilisation de l'ensemble de la chaîne de production » (janvier 2019).

9 « Millions of Americans' Medical Images and Data Are Available on the Internet. Anyone Can Take a Peek », *ProPublica*, 17 septembre 2019.

10 Selon la définition de la Commission nationale de l'Informatique et des Libertés, *« cette notion recouvre non seulement l'ensemble des données collectées et produites dans le cadre du parcours de soins mais aussi celles qui, détenues par d'autres acteurs (développeurs d'application par exemple), constituent une information sur l'état de santé de la personne »*.

11 C'est par exemple le cas des données relatives aux « pathologies discriminantes », comme les maladies mentales.

12 « Cybersécurité : vers la responsabilisation de l'ensemble de la chaîne de production », Renaissance Numérique, janvier 2019.

13 Intitulée « Cybersécurité : vers un système de santé résilient ? », la table ronde s'est tenue à Paris et a rassemblé :

- Gilles Castéran, Directeur exécutif, Accenture Security France ;
- Stéphane Pierrefitte, Directeur des systèmes d'information, GHU Paris Psychiatrie et Neurosciences ;
- Annabelle Richard, Avocate associée, Pinsent Masons ;
- Bertrand Trastour, Responsable des activités BtoB, Kaspersky France.

Cette note s'inspire librement des échanges lors de ce débat pour porter le point de vue de Renaissance Numérique.

14 Une analyse détaillée de la chronologie de la stratégie « Ma Santé 2022 » et du contenu de la loi est disponible sur le site de l'Institut de recherche et documentation en économie de la santé.

PARTIE 1

UNE CHAÎNE DE VALEUR FACE À DES CONTRAINTES PARTICULIÈREMENT ÉLEVÉES EN MATIÈRE DE CYBERSÉCURITÉ

UN SECTEUR FRAGILISÉ PAR SA PROFONDE HÉTÉROGÉNÉITÉ

À la différence de secteurs comme la banque ou les assurances, qui font également face à une menace croissante mais dont les conséquences sont principalement financières, une cyberattaque d'envergure qui ciblerait un établissement de soins peut mettre en péril des vies humaines.

> *« Dans un contexte où la menace est de plus en plus sophistiquée, ciblée et destructive, le secteur de la santé est largement exposé au regard de ses spécificités : forte décentralisation, forte diversification et accélération de la transformation digitale qui sont par ailleurs et incontestablement ses forces. »*
>
> **GILLES CASTÉRAN,**
> **Directeur exécutif, Accenture Security France**[15]

Or, la chaîne de soins se caractérise par une très grande hétérogénéité de structures (centres hospitaliers, médecins de ville, laboratoires, cabinets d'infirmiers, prestataires logistiques, techniques, etc.) et de métiers (deux cents métiers différents, soit plus de deux millions de professionnels[16]) qui ne disposent pas tous de la même maturité numérique. Ces inégalités sont entre autres susceptibles d'être renforcées par la situation géographique, la taille et les capacités financières propres à chaque acteur. Deux autres facteurs tendent à complexifier davantage les tâches de sécurisation dans ce secteur : le caractère décentralisé de l'écosystème de santé et l'hyperconnexion d'un grand nombre de systèmes industriels différents (ex. : les dispositifs médicaux intégrant du logiciel, en très forte augmentation). Cette hyperconnexion est renforcée à la fois par l'entrée de nouveaux acteurs qui font des données médicales le cœur de leur modèle d'affaires, et l'accélération des initiatives de rapprochements entre établissements de santé.

15 Citation issue de l'intervention de Gilles Castéran lors de la table-ronde organisée par Renaissance Numérique le 25 octobre 2019.
16 « Les chiffres-clés de l'offre de soins », DREES, 2018.

D'après Tanguy de Coatpont, Directeur général de Kaspersky France, *« historiquement, l'essor de l'informatique dans les établissements de santé a conduit les praticiens à imposer leurs habitudes et appareils numériques personnels à leur Direction des Services d'Information. La pratique du « bring your own device » (BYOD) était même parfois plébiscitée par les responsables eux-mêmes car moins coûteuse que la mise à jour du parc complet des équipements »*[17]. Faute de financements suffisants et d'une stratégie commune, certains établissements se sont retrouvés, au tournant des années 2010, avec des services d'information (SI) peu efficients, voire obsolètes (cf. la présence encore importante des OS Windows XP et Windows 7 dans les parcs informatiques, le premier n'étant plus mis à jour par Microsoft depuis 2014, le second depuis le 14 janvier 2020). Ainsi, la migration informatique dans un secteur décentralisé qui compte des dizaines de milliers de terminaux connectés n'est parfois pas suffisamment rapide pour prévenir les risques relatifs aux failles de sécurité.

Outre ces difficultés structurelles, les acteurs de la santé doivent se conformer à un cadre réglementaire particulièrement fourni en matière de cybersécurité, cadre qui s'est renforcé au cours des quatre dernières années.

17 D'après une étude menée par Kaspersky France/Yougov et intitulée « Protection des données de santé : du curatif au préventif », octobre 2019.

UN CADRE RÉGLEMENTAIRE AU SEIN DUQUEL SE CHEVAUCHENT DIFFÉRENTS ENJEUX DE CYBERSÉCURITÉ

Un cadre spécifique régit la collecte, le traitement, l'hébergement et la sécurisation des données manipulées par les acteurs du parcours de soins. En effet, du fait du caractère particulièrement sensible de ces données, les législateurs français et européen ont progressivement étoffé l'arsenal juridique pour protéger les patients et garantir la confidentialité de leurs informations numériques. Dans les faits, les acteurs de la santé doivent se conformer à un grand nombre de textes plus ou moins généraux et complexes à appréhender (voir le Tableau 1), au premier rang desquels figure le règlement général sur la protection des données (RGPD). La loi relative à l'organisation et à la transformation du système de santé qui a été publiée au Journal officiel le 26 juillet 2019 offre également un nouveau cadre juridique en matière de pilotage des données de santé. Elle prévoit de remplacer l'Institut national des données de santé (INDS) par une plateforme numérique des données de santé (le *Health Data Hub*). Ainsi, au 1er janvier 2022, tout patient disposera d'un espace numérique de santé. Cet espace contiendra d'une part l'accès au dossier médical personnel, d'autre part, tout patient aura accès à ses données administratives et à ses données dites « constantes de santé » qui peuvent, notamment, être collectées via les services destinés à la coordination des parcours de santé ou les objets connectés.

Par ailleurs, la transposition de la Directive « Network and Information System Security » (NIS) en droit français prévoit la désignation d'une liste d'« opérateurs de services essentiels » (OSE) auxquels s'appliquent des règles supplémentaires en matière de cybersécurité. Le décret publié au Journal officiel en mai 2018 cite en annexe les services *« concourant aux activités de prévention, de diagnostic ou de soins »*, *« la réception et la régulation des appels »* et *« le service mobile d'urgence et de réanimation »* dans le cadre de l'aide médicale d'urgence, ainsi que la « *distribution pharmaceutique* ». Les services de calcul et paiement des prestations sociales (assurance maladie, vieillesse, allocations familiales et chômage) font également partie des OSE. Cette définition est toutefois théorique et son champ d'application manque de clarté. En effet, si les responsables des centres hospitaliers ont tout de suite compris que leurs activités étaient concernées, un certain nombre d'autres acteurs qui traitent des données de santé mais qui ne se considèrent pas à première

vue comme des acteurs de santé – dans le sens où ils ne fournissent pas de diagnostic ou de traitement médical à proprement parler – peuvent se poser la question de savoir si ces dispositions s'appliquent à eux ou non.

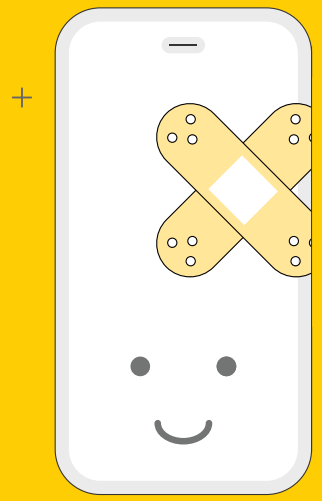
TABLEAU 1 - LES PRINCIPAUX TEXTES RELATIFS À LA CYBERSÉCURITÉ DANS LE CHAMP DE LA SANTÉ

Champ d'action	Textes associés
Obligations de sécurité des « opérateurs de services essentiels » dont font partie les établissements de soins (ce qui inclut les hôpitaux et cliniques privées)	**Directive « Network and Information System Security » (NIS)** (UE 2016/1148 du 6 juillet 2016)
	Loi de transposition (loi n°2018-133 du 26 février 2018)
	Décret d'application (Décret n° 2018-384 du 23 mai 2018)
Réglementation concernant le traitement et la mise à disposition des données	**Règlement général sur la protection des données** (article 9 sur le traitement de données sensibles)
	Loi Informatique et Libertés (Loi n° 78-17 du 6 janvier 1978) notamment ses chapitres IX et X
	Code de la santé publique (Art. L. 1460-1 et suivants)
	Loi relative à l'organisation et à la transformation du système de santé (Loi n° 2019-774 du 24 juillet 2019) notamment la modification des articles L1110-4-1 et L1462-1 du Code de la santé publique et la création de l'article L6316-2 du même Code
Règles en matière d'hébergement de données de santé et de signalements d'incidents de sécurité	Code de la santé publique (Art. L1111-8 à L1111-8-2 et Art. D1111-16-2 à D1111-16-4)
Dispositions relatives aux référentiels de sécurité et d'interopérabilité des données de santé	Code de la santé publique (Art. L. 1110-4-1)

Parmi les obligations spécifiques qui s'appliquent aux OSE figurent, par exemple, la désignation d'un représentant auprès de l'ANSSI ou la notification à l'agence, sans délai après en avoir pris connaissance, des « *incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de services essentiels, lorsque ces incidents ont ou sont susceptibles d'avoir, compte tenu notamment du nombre d'utilisateurs et de la zone géographique touchés ainsi que de la durée de l'incident, un impact significatif sur la continuité de ces services* » (arrêté du 13-6-2018, art. 3). Cela ne concerne donc pas uniquement les données de santé et dans la pratique il existe un risque de chevauchement avec les obligations au titre du RGPD et de la loi Informatique et Libertés. Une structure de soins (hôpital, clinique privée, etc.) peut se retrouver dans une situation consécutivement à un incident de sécurité pour lequel elle doit faire une notification officielle auprès de l'ANSSI, mais pas à la Commission nationale de l'Informatique et des Libertés (CNIL), un cas où elle est débitrice de cette obligation de déclaration aux deux autorités – sachant qu'elles ne demanderont pas nécessairement les mêmes informations, ni dans les mêmes délais ou les mêmes procédures – et que chacune est susceptible de déclencher à posteriori son propre mécanisme d'investigation complémentaire. Ces nouvelles dispositions – et les coûts d'application associés – concernent tous les OSE, des grands centres hospitaliers aux cliniques de taille plus modeste, avec des capacités de mise en conformité rapide nécessairement variables. Afin de permettre aux professionnels de santé de naviguer efficacement dans la myriade de dispositions réglementaires applicables en matière de cybersécurité, l'Agence du numérique en santé (ex-ASIP) et le ministère mettent notamment à disposition un portail avec un grand nombre d'informations pratiques et des référentiels d'application (https://www.cyberveille-sante.gouv.fr/). Cette initiative participe des efforts d'information et de sensibilisation des professionnels du secteur.

PARTIE 2

ADAPTER LA CULTURE DE LA GESTION DE CRISE SANITAIRE À L'ÈRE NUMÉRIQUE



UNE CAPACITÉ D'ADAPTATION INHÉRENTE AU SECTEUR

Si le numérique se diffuse aujourd'hui largement dans le quotidien des personnels de santé (ex. : gestion des prises de rendez-vous en ligne, DMP, télémédecine, etc.), la structuration des systèmes d'information et les réflexions autour de la gouvernance des données sont, elles, relativement récentes. L'un des objectifs de la stratégie nationale « Ma Santé 2022 », qui s'accompagne d'un plan de financement dédié, est de fournir aux établissements de soins un cadre harmonisé, piloté par la nouvelle Agence du numérique en santé. Cette agence est notamment chargée de *« l'élaboration des référentiels de sécurité (PGSSI-S) et d'interopérabilité (CI-SIS), elle met aussi à disposition des services d'authentification (Pro-santé Connect, e-CPS) et de cybersurveillance et favorise la généralisation des messageries sécurisées de santé»*[18].

Cette étape d'harmonisation est cruciale face à l'augmentation de la menace. De par sa vocation, le secteur n'est toutefois pas étranger à la gestion des risques et dispose de plusieurs atouts pour rattraper ce retard.

> *« Les établissements de santé disposent d'une magnifique plasticité organisationnelle et opérationnelle, qui leur permet de s'adapter à l'ensemble des nouveaux enjeux qui s'ouvrent à eux, tant territoriaux, que populationnels ou de cybersécurité. Ces établissements en qualité d'opérateur de service essentiel (OSE) se préparent à la montée des cyberattaques. Ils se dotent de politique de sécurisation à la mesure des dangers auxquels ils sont et seront exposés dans le cadre de la poursuite de leur démarche continue de gestion des risques. »*
>
> **STÉPHANE PIERREFITTE,**
> **Directeur des systèmes d'information, Groupement hospitalier universitaire Paris Psychiatrie et Neurosciences[19]**

18 Voir sur le site de l'institution : https://esante.gouv.fr/actualites/lasip-sante-devient-lagence-du-numerique-en-sante

19 Citation issue de l'intervention de Stéphane Pierrefitte lors de la table-ronde organisée par Renaissance Numérique le 25 octobre 2019.

La notion de « plasticité organisationnelle » prend effectivement tout son sens lorsqu'elle est appliquée au secteur de la santé. Les professionnels sont déjà rompus (bon gré mal gré) à un rythme de réformes particulièrement soutenu. De plus, les établissements de soins – au premier rang desquels une partie du monde hospitalier – disposent de fortes aptitudes en matière de gestion de crise, avec une large palette de processus déjà en place en cas d'incident majeur. Cela passe par l'organisation d'exercices de mise en situation, la mise à disposition d'outils non-électroniques (ex. : pour pouvoir ventiler un patient à la main ou effectuer une opération sans assistance technique), de moyens de communication non-numériques (ex. : radios VHF, listes papier de contacts mises à jour régulièrement). Les personnels de ces établissements sont également formés pour assurer le plus de services de soins possible en cas de « crise ». Cette capacité de résilience n'est pas uniquement utile dans l'hypothèse d'une coupure de courant généralisée ou en situation de guerre : c'est aussi un atout en cas de cyberattaque d'envergure touchant directement les fonctions principales d'un centre de soins.

Les soignants, conformés aux règles d'hygiène dans leur pratique quotidienne, doivent désormais étendre leur vigilance aux « règles élémentaires d'hygiène numérique »[20]. Cela nécessite de déployer des efforts de sensibilisation à la fois au sein des établissements de soins et des instances de coopération inter acteurs.

20 Pour reprendre l'expression de Guillaume Poupard, Directeur général de l'ANSSI.

LA FORMATION ET LA MISE EN COMMUN DES EFFORTS DE SÉCURISATION : DEUX FACTEURS CLEFS D'UNE CYBER-RÉSILIENCE PARTAGÉE

« Je ne suis pas d'accord avec l'idée reçue selon laquelle l'utilisateur est systématiquement le maillon faible en matière de sécurité informatique car il est potentiellement le maillon le plus fort, mais à condition qu'il soit éduqué, qu'on l'ait amené à prendre conscience des conséquences de ses actes. C'est de l'éducation, car, pour un médecin, un personnel soignant ou administratif, dans ses actes quotidiens « fermer sa session » peut être considéré comme un acte sans intérêt, comme une perte de temps. Il faut donc lui donner la bonne information pour qu'il l'intègre dans son schéma quotidien. C'est cela la cybersécurité, ce n'est pas uniquement empiler des couches de solutions informatiques, c'est avant tout travailler sur l'humain et c'est finalement là où nous avons le plus gros potentiel de développement aujourd'hui. »

BERTRAND TRASTOUR,
Responsable des activités BtoB, Kaspersky France[21]

La formation de l'ensemble des professionnels de santé – pas uniquement le personnel soignant, mais aussi tous les métiers qui manipulent l'informatique au quotidien – et la sensibilisation des patients est la priorité absolue pour garantir un niveau de sécurisation optimal. Depuis octobre 2017, le gouvernement français a mis à disposition le portail « Cybermalveillance.gouv.fr » qui propose notamment un kit de sensibilisation recensant les bonnes pratiques en matière d'hygiène numérique[22]. Cet outil mériterait d'être largement partagé auprès des acteurs qui interviennent dans le système de santé.

21 Citation issue de l'intervention de Bertrand Trastour lors de la table-ronde organisée par Renaissance Numérique le 25 octobre 2019.

22 Le kit inclut par exemple « *10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe* », des mesures préventives vis-à-vis des rançongiciels, ainsi qu'un quizz pour tester ses connaissances. Le kit complet est accessible à cette adresse : https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/

Ces efforts de sensibilisation requièrent du temps et de l'investissement à des professionnels qui sont déjà particulièrement sollicités au quotidien. Ils sont pourtant un passage obligatoire, au risque de compromettre sérieusement les efforts techniques déployés par les responsables des systèmes d'information dans un contexte de menace croissante.

Dans un secteur de la santé en pleine transition numérique accélérée, cette sensibilisation passe également par une prise de conscience de la valeur des données, et pas uniquement celles à caractère médical mais également, à titre d'exemple, celles générées par les laboratoires de recherche ou les applications de « bien-être[23] ». Toutes ces données virtuelles sont en réalité valorisables pour un certain nombre d'acteurs (cf. les montants de revente d'un dossier médical sur le *dark web* ou les *ransomwares*), ce qui les ancre dans des logiques économiques bien réelles.

« Il est primordial que les efforts de sensibilisation incluent tout le monde, car la cybersécurité concerne l'ensemble des métiers de la santé. Les méthodes d'approche « par le jeu » sont un excellent véhicule pour améliorer l'implication des participants et, par le biais de leur compétitivité naturelle, les pousser à participer. Des communications régulières sur la réalité des risques, pour chaque groupe ou métier spécifiquement, peuvent aussi aider à la responsabilisation et à l'adhésion. Cela ne doit pas rester uniquement théorique, il est nécessaire de faire des mises en situation régulières pour entraîner le « muscle » de la gestion de crise. »

ANNABELLE RICHARD
Avocate associée, Pinsent Masons[24]

23 Ces données, collectées principalement via des objets connectés (ex. : bracelet) reliés à une application installée sur smartphone, peuvent - par exemple - être revendues par les éditeurs à des laboratoires pharmaceutiques afin d'obtenir des données en vie réelle.

24 Citation issue de l'intervention d'Annabelle Richard lors de la table-ronde organisée par Renaissance Numérique le 25 octobre 2019.

Si plusieurs établissements de soins mettent déjà en place des politiques de formation et des exercices de mise en situation afférents à ces enjeux, les capacités de mise en oeuvre de ces politiques sont extrêmement hétérogènes au sein du système de santé. Par ailleurs, historiquement, les établissements de soins ont conçu, pour la plupart, leurs infrastructures SI en vase clos, sans réelle politique d'homogénéisation inter acteurs. Cela a conduit à une fragmentation de l'écosystème actuel, avec notamment des difficultés liées à l'interopérabilité des systèmes qui complexifient le partage de données entre établissements (ex. : entre un laboratoire d'analyse médicale, un EHPAD et un CHU). À ce titre, plusieurs initiatives existent depuis avril 2016 et la parution du décret encadrant la constitution des groupements hospitaliers de territoire (GHT) et la convergence de leurs systèmes d'informations, dont l'un des bénéfices attendus est la mise en place de politiques communes en matière de sécurité. La logique de décloisonnement figure également au cœur du plan « Ma Santé 2022 », qui renforce les communautés professionnelles territoriales de santé (CPTS)[25] avec l'objectif de créer un millier de ces communautés d'ici à 2022. Cette phase de transition vers davantage de coopération inter acteurs peut être l'occasion de réfléchir collectivement aux enjeux de cybersécurité et réaliser une « mise à jour » partagée des procédures de sécurisation des systèmes d'information. Les CPTS pourraient, par exemple, servir de lieux de dialogue et de sensibilisation autour de ces enjeux, voire d'organisation d'exercice de gestion de crise à l'échelle d'un territoire, sous la houlette de structures « chefs de file » particulièrement avancées en matière de cybersécurité (à l'instar de certains groupements hospitaliers).

Toutefois, la chaîne des soins ne se résume pas aux seuls professionnels de santé et les cyber risques appellent à une coopération et vigilance auprès d'autres acteurs, notamment dans la mise en oeuvre des relations contractuelles. Pour illustration, le RGPD encourage, entre autres, les établissements de soins à insérer des clauses d'audit dans les contrats qui les lient à leurs prestataires de services informatiques[26]. Ainsi, outre la nécessité de prévoir tous les aspects liés à la maintenance des solutions informatiques (mises à

25 Selon le site internet de l'Agence régionale de santé du Centre-Val-de-Loire, «*chaque CPTS a vocation à réunir des professionnels de premier et de deuxième recours (médecins généralistes et d'autres spécialités, infirmières, etc.), et, le cas échéant, des acteurs médico-sociaux ou sociaux, qui interviennent ensemble pour fluidifier le parcours de soins des patients. Son objectif est de renforcer les liens entre professionnels et de proposer, dans son projet de santé, des actions et outils de coordination* ».

26 Un exemple de contrat de sous-traitance prévoyant des clauses d'audit est accessible sur le site web de la CNIL.

jour, responsabilité en cas d'incident, délais d'intervention, etc.), il est conseillé de réaliser des audits à intervalle régulier. Avec suffisamment de préparation en amont (quels détails demander, quel intervalle entre deux audits et quel délai de notification, qui prend en charge les frais, etc.), cet outil permet de s'assurer qu'un prestataire applique bel et bien ses engagements et que ses activités sont adaptées aux types de données traitées. L'enjeu est désormais de n'omettre aucun des maillons de la chaîne de santé dans les procédures de sécurisation, jusqu'au patient.

CONCLUSION

DE LA NÉCESSAIRE SOLIDARITÉ ENTRE LES MAILLONS DE LA CHAÎNE DE SOINS

Les enjeux de cybersécurité revêtent une dimension particulière quand on l'applique au secteur de la santé. Face à une menace grandissante et un cadre réglementaire qui s'est largement étoffé ces dernières années, les établissements de soins sont contraints à réinventer leur rapport aux données et à revoir les modèles de partage avec leurs prestataires mais également les patients.

Malgré l'hétérogénéité des acteurs qui composent l'écosystème de santé, le plus grand atout du secteur réside dans sa capacité à s'adapter au changement. Pour accélérer cette mutation, l'accent doit toutefois être mis sur la formation de tous les métiers du parcours de soins aux enjeux de cybersécurité, en capitalisant sur les ressources existantes (ex. : kits de sensibilisation, référentiels) et l'expertise déjà présente dans certaines structures « modèles ». Par ailleurs, les chantiers de rapprochement et de mutualisation entre établissements de santé, initiés par les pouvoirs publics depuis 2016 et renforcés par le plan « Ma Santé 2022 », sont sans doute des opportunités à saisir pour renforcer la cyber-résilience de l'ensemble de la chaîne.

TROIS RECOMMANDATIONS POUR UN SYSTÈME DE SANTÉ RÉSILIENT

1 SENSIBILISER TOUS LES ACTEURS DU PARCOURS DE SOINS AUX ENJEUX DE CYBERSÉCURITÉ

Ces efforts de sensibilisation doivent être réalisés dès la formation initiale des professionnels de santé, puis tout au long de leur carrière professionnelle. Ils doivent également intégrer les autres acteurs de la chaîne, jusqu'aux prestataires et aux patients. Cette démarche de sensibilisation doit être alimentée dans la durée, afin de s'adapter à des risques mouvants.

2 SÉCURISER L'ENSEMBLE DE LA CHAÎNE DE SANTÉ EN CONSOLIDANT LES RELATIONS CONTRACTUELLES ENTRE ÉTABLISSEMENTS DE SOINS ET PRESTATAIRES

Cela peut passer, entre autres, par l'élaboration ou le renforcement des clauses relatives aux audits des processus internes mis en place par les prestataires qui manipulent des données de santé (ex. : prévoir la fréquence de ces audits, une grille des éléments à vérifier, les détails relatifs à la prise en charge des frais associés, etc.).

3 MISER SUR DES ÉTABLISSEMENTS DE SOINS « CHEFS DE FILE » POUR DIFFUSER LES BONNES PRATIQUES EN MATIÈRE D'HYGIÈNE NUMÉRIQUE AU SEIN DES TERRITOIRES

Par exemple, un CHU particulièrement en pointe sur les méthodes de gestion de crise pourrait participer de l'accompagnement d'autres établissements moins bien dotés avec lesquels il collabore sur un même territoire. Le nouvel échelon qu'est la CPTS pourrait également être un lieu d'échanges afin de sensibiliser les acteurs du parcours de soins aux enjeux de cybersécurité et effectuer des exercices de gestion de crise inter acteurs.

POUR ALLER PLUS LOIN

“Cybersécurité : vers la responsabilisation de l’ensemble de la chaîne de production”, Renaissance Numérique (janvier 2019).

“17 Experts / 36 propositions pour une ambition politique en matière de e-santé”, Renaissance Numérique (mars 2017).

“D’un modèle de santé curative à un modèle préventif grâce aux outils numériques”, Renaissance Numérique (septembre 2014).

DIRECTION DE LA PUBLICATION

Henri Isaac, Président de Renaissance Numérique

Jennyfer Chrétien, Déléguée générale de Renaissance Numérique

RAPPORTEUR

Ruben Narzul

Nous remercions pour leurs contributions Bernard Astruc, Directeur des affaires médicales d’Eutelmed et Annabelle Richard, Avocate associée chez Pinsent Masons. médicales d’Eutelmed et Annabelle Richard, Avocate associée chez Pinsent Masons.

RENAISSANCE
numerique

À PROPOS DE RENAISSANCE NUMÉRIQUE

Renaissance Numérique est le principal think tank français indépendant dédié aux enjeux de transformation numérique de la société. Réunissant des universitaires, des associations, des grandes entreprises, des start-ups et des écoles, il vise à élaborer des propositions opérationnelles pour accompagner les acteurs publics, les citoyens et les acteurs économiques dans la construction d'une société numérique inclusive.

Renaissance Numérique
22 bis rue des Taillandiers - 75011 Paris
www.renaissancenumerique.org

Février 2020