Cyberattaques contre les systèmes d'information de santé au Canada

Vinyas Harish BCompH, Alun Ackery MD MSc, Kiran Grant MD, Trevor Jamieson MD MBI, Shaun Mehta MD GPLLM

■ Citation : *CMAJ* 2023 November 20;195:E1548-54. doi : 10.1503/cmaj.230436-f

Voir la version anglaise de l'article ici : www.cmaj.ca/lookup/doi/10.1503/cmaj.230436

Au Canada, la numérisation des systèmes de santé a connu un essor considérable. En 2019, 86 % des médecins de famille canadiens interrogés ont déclaré utiliser des dossiers médicaux électroniques (DMÉ)[1]. Les outils numériques pour les soins virtuels, la surveillance à distance de l'état de la patientèle, les dispositifs portables, les plateformes de coordination des soins et l'Internet des objets (IdO) se répandent dans la pratique[2]. La numérisation et l'intégration sur des réseaux partagés de systèmes disparates d'information sur la santé promettent d'améliorer la commodité, l'accès et la qualité des soins, mais peuvent introduire un risque pour la patientèle, les prestataires de soins et les systèmes de santé. Bien que certains prestataires de soins de santé aient reçu une formation spécialisée en technologies de l'information (TI), ce n'est pas le cas de la plupart d'entre eux, et évoluer dans des systèmes d'information de santé de plus en plus complexes peut provoquer un stress intense.

Les cyberattaques peuvent entraîner des atteintes à la vie privée et des préjudices financiers. Ils peuvent également compromettre la sécurité de la patientèle et le fonctionnement des systèmes de santé. Les renseignements personnels sur la santé (RPS) peuvent atteindre des prix beaucoup plus élevés sur le Web invisible que d'autres informations personnelles (p.ex., l'information sur les cartes de crédit)[3]. Une enquête internationale menée en 2021 auprès de décideurs en technologies de la santé a conclu que le coût moyen d'une attaque par rançongiciels était de 1,27 million de dollars américains[4]. Les cyberattaques contre les systèmes d'information de santé ont été associées à des retards dans les soins, au transfert de patients et patientes vers d'autres sites et à une augmentation de la mortalité[5]. Au Canada, ces attaques sont de plus en plus fréquentes; 48 % de toutes les brèches de sécurité signalées en 2019 s'étant produites dans le secteur de la santé[6]. Les cyberattaques se sont également multipliées dans un contexte marqué par des événements tels que la pandémie de COVID-19 et la guerre russo-ukrainienne[7,8]. Ici, nous présentons les répercussions des cyberattaques sur les systèmes d'information de santé du Canada et expliquons comment les prestataires de soins de santé, qu'ils exercent dans de grands hôpitaux ou dans des cabinets individuels, peuvent améliorer leurs mesures de cybersécurité.

Points clés

- Les cyberattaques peuvent entraîner des atteintes à la vie privée et des préjudices financiers. Ils peuvent également compromettre la sécurité de la patientèle et le fonctionnement des systèmes de santé.
- La réduction du risque de cyberattaques et la gestion de celles qui surviennent se déroulent en 4 étapes : prévention, détection, intervention et redressement.
- À mesure que de nouveaux domaines de cybermenaces émergent (p. ex., les appareils connectés à Internet), les prestataires de soins de santé et les organismes de santé devraient surveiller les rappels, maintenir leurs logiciels à jour et discuter des risques possibles avec leur patientèle.
- Le maintien de l'efficacité des flux de travail et la mise en œuvre de pratiques exemplaires en cybersécurité impliquent des compromis; cependant, les inconvénients mineurs des mesures de sécurité telles que l'authentification à 2 facteurs pour se connecter sont nettement préférables au redressement opérationnel après une cyberattaque.

Comment les cyberattaques ont-elles affecté les systèmes d'information de santé au Canada?

Les cyberattaques contre les systèmes d'information de santé prennent le plus souvent la forme de rançongiciels ou d'atteintes à la vie privée (figure 1). Depuis 2015, au moins 14 cyberattaques majeures contre des systèmes d'information de santé ont eu lieu, dont 9 tentatives de rançon et 6 compromettant les RPS. Les attaques par rançongiciel commencent par l'installation ou l'activation d'un logiciel malveillant (un maliciel) qui verrouille ou crypte un système informatique et les données qui y sont stockées jusqu'à ce qu'une rançon soit versée. Mais l'accès aux données est souvent perdu, même lorsque la rançon est payée[4]. L'attaque peut également entraîner des atteintes à la vie privée, par l'exfiltration des RPS des systèmes d'information de santé et leur distribution illicite sur des marchés en ligne. Les attaques par déni de service sont une autre forme d'extorsion, par laquelle un attaquant submerge un site Internet en créant une fausse affluence qui le rend inaccessible aux utilisatrices et aux utilisateurs réels (p. ex., la patientèle souhaitant prendre rendez-vous) jusqu'à ce qu'un

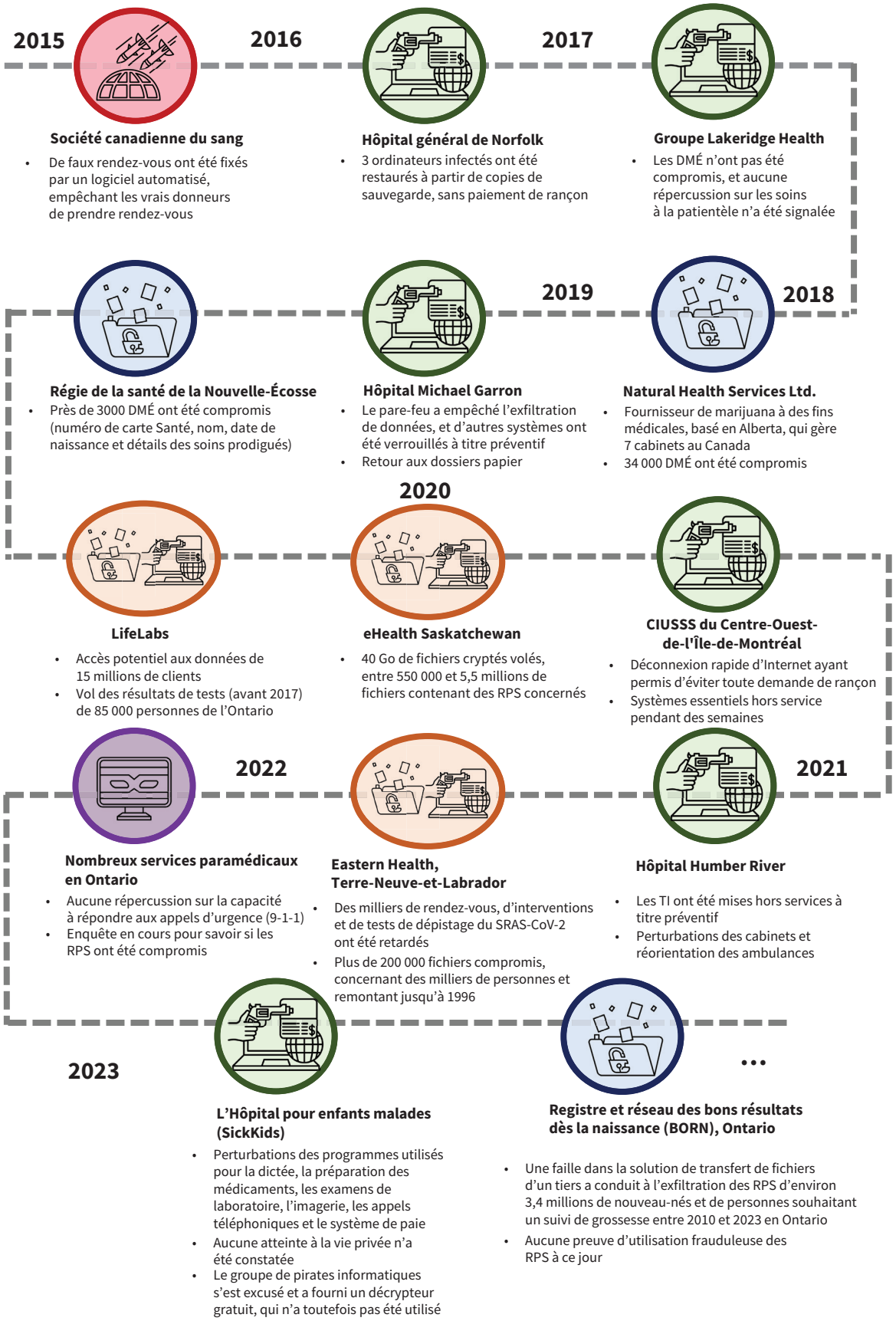

Figure 1 : Cyberattaques récentes contre des systèmes d'information de santé au Canada, y compris par déni de service (rouge), rançongiciel (vert), atteintes à la vie privée (bleu), attaques mixtes (orange) et attaques de type non identifié (violet). Remarque : CIUSSS = centre intégré universitaire de santé et de services sociaux, DMÉ = dossiers médicales électronique, TI = technologies de l'information, RPS = renseignements personnels sur la santé.

paiement soit effectué[9]. Bien que la plupart des cyberattaques contre les organismes de santé soient imputables à des personnes criminelles, elles peuvent également être commanditées par des États-nations, des groupes terroristes, des « cyberactivistes » et des extrémistes violents à motivation idéologique (p. ex., les personnes qui ciblent les centres d'avortements)[10–12].

Les organismes de santé, quelle que soit leur taille, sont des cibles idéales pour les cyberattaques. Tout d'abord, elles sont des cibles lucratives du fait de la valeur des RPS, et elles disposent probablement aussi de ressources suffisantes pour payer des rançons. Comme les personnes cybercriminelles adaptent le montant de la rançon à la capacité présumée qu'a la cible de payer, elles peuvent s'attendre à être capables d'obtenir un montant de l'ordre de Can$3000–Can$5000 en échange des systèmes d'information de santé de cabinets individuels de médecins[13]. Aucun paiement de rançon par un hôpital canadien n'a été rapporté à ce jour, mais les systèmes de santé des États-Unis ont déjà payé des rançons de plusieurs millions de dollars[14]. Même si aucune somme n'est versée, la tentative d'extorsion peut entraîner de longues périodes d'indisponibilité des systèmes d'information de santé, et donc des répercussions importantes (et fortement médiatisées) sur les technologies de l'information et les services destinés à la patientèle. Par ailleurs, la vaste couverture médiatique des cyberattaques contre les systèmes de santé accroît la pression sur les victimes, poussées à payer les rançons avant que la situation ne soit rendue publique. De plus, les organismes de santé investissent souvent trop peu dans les systèmes informatiques et utilisent des systèmes obsolètes ou archaïques qui sont vulnérables aux attaques. Enfin, les organismes de santé ne disposent pas toujours des moyens nécessaires pour contrer les cybermenaces, ce qui amplifie les dommages causés par le piratage ainsi que la probabilité qu'ils paient les rançons.

Quelles leçons le Canada peut-il tirer des pratiques de pays pairs en matière de cybersécurité?

Il est difficile de faire une comparaison exhaustive des conséquences des attaques sur différents territoires, car de nombreuses cyberattaques contre les systèmes d'information de santé ne sont pas signalées[15]. Bien que les stratégies et pratiques exemplaires en cybersécurité des utilisatrices et utilisateurs finaux (routines quotidiennes, bonnes pratiques et contrôles ponctuels, des pratiques qu'on pourrait comparer aux habitudes d'hygiène personnelle) soient essentiellement les mêmes au sein de tous les organismes, secteurs et pays, la politique de cybersécurité au Canada pourrait encore être considérablement améliorée.

En juin 2022, la Chambre des communes a déposé un projet de *Loi sur la protection des cybersystèmes essentiels* (LPCE), qui définit les cybersystèmes essentiels comme ceux dont la compromission aurait des conséquences graves pour la sécurité publique. Ces systèmes jouent un rôle dans les domaines des télécommunications, des pipelines, de l'énergie nucléaire, des transports réglementés par le gouvernement fédéral et des banques, mais pas les organismes de santé[16]. Aux États-Unis, en revanche, l'Agence américaine de cybersécurité et de sécurité des infrastructures (United States Cybersecurity and Infrastructure Security Agency ou CISA) soutient une multitude de conseils de coordination sectoriels qui collaborent avec le gouvernement pour partager l'information et assurer la coordination et la mise en place sur une base volontaire de pratiques visant à promouvoir la résilience. Le Conseil de coordination du secteur des soins de santé et de la santé publique (Healthcare and Public Health Sector Coordinating Council) compte des dizaines de membres, dont des systèmes de santé, des groupes de défense, des assureurs et des organismes à but non lucratif[17]. Bien que l'exclusion des organismes de santé de la LPCE puisse être considérée comme conforme aux principes fédéraux–provinciaux de la Loi canadienne sur la santé, des mécanismes de gouvernance tels que les conseils de coordination sectoriels pourraient promouvoir l'adhésion à des normes communes tout en encourageant l'innovation et l'expérimentation.

Il existe une grande hétérogénéité dans les mesures de cybersécurité prises par les organismes du secteur public au sens large selon les provinces et les territoires, car les institutions de plus petite envergure n'ont souvent pas les ressources financières et humaines nécessaires. Les modèles de services partagés peuvent contribuer à remédier à ces disparités. Par exemple, l'organisme Santé Ontario, créé par le gouvernement ontarien, pilote 6 centres régionaux d'opérations de sécurité[18]. Chaque centre surveille en permanence les pratiques de sécurité des institutions membres, les défend contre les brèches de sécurité, et isole et atténue de manière proactive les risques de sécurité. Ces centres sont semblables aux équipes d'intervention en cas d'urgence informatique dans le domaine de la santé qui ont été bien accueillies en Norvège, aux Pays-Bas et au Royaume-Uni[10]. À mesure que les gouvernements mettent en place ces instances, les prestataires de soins de santé et les organismes de santé doivent se familiariser avec elles et avec leur système de signalement d'incidents et de recours hiérarchique. Les gouvernements doivent également s'efforcer de mobiliser les prestataires de soins de santé au moment de mettre en place ces instances afin de veiller à ce que leurs besoins et leurs points de vue soient pris en compte. Les provinces et les territoires devraient faire preuve de prudence quant à la réglementation des pratiques de cybersécurité en sus du signalement effectué par les prestataires de soins ou les organismes de santé (p. ex., en imposant des audits semestriels de cybersécurité), car les exigences imposées par les échelons hiérarchiques supérieurs peuvent être trop onéreuses en matière d'efforts, de capital et de ressources humaines, en particulier pour les petites structures. En outre, les provinces et les territoires devraient établir des répertoires publics des cyberattaques menées contre les systèmes d'information de santé[15]. Ces répertoires pourraient constituer une aide précieuse à la recherche et orienter les choix de la patientèle, qui pourrait préférer les prestataires de soins de santé ayant de solides antécédents en matière de cybersécurité.

Comment les prestataires de soins de santé peuvent-ils prévenir les cyberattaques et les contrer?

L'Institut national des normes et de la technologie (National Institute of Standards and Technology) des États-Unis décrit

Pratiques de cybersécurité pour les médecins du Canada

Mesures de réduction des risques de cyberattaque à prendre par les médecins et les prestataires de soins de santé travaillant dans des cabinets ou des hôpitaux

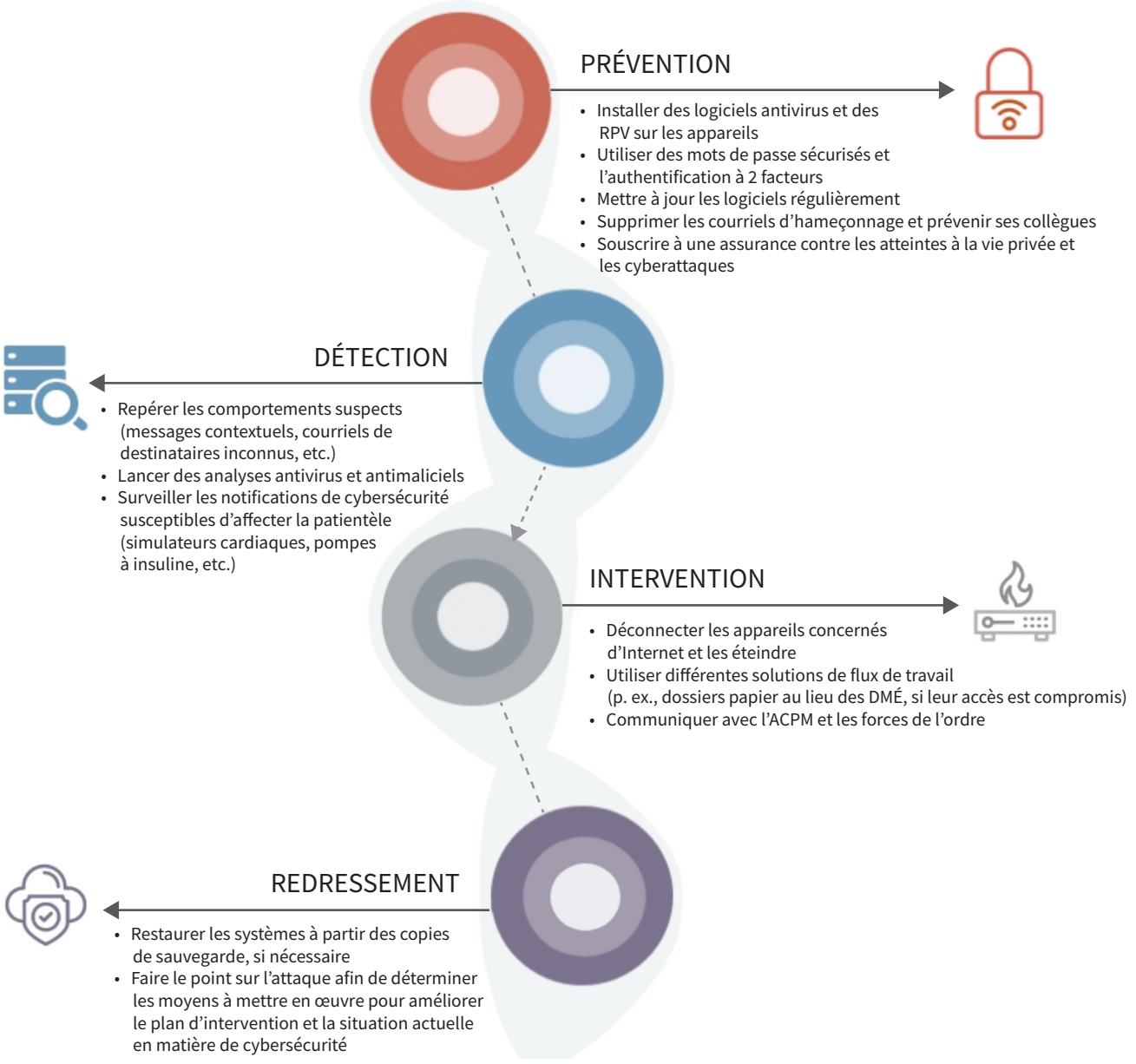

Figure 2 : Quatre phases de la cyberrésilience, et les mesures recommandées. Remarque : ACPM = Association canadienne de protection médicale, DMÉ = dossier médical électronique, RPV = réseau privé virtuel.

5 phases pour contrer efficacement les cyberattaques : observation, protection, détection, intervention et redressement[19]. Par souci de simplicité, nous avons combiné les étapes d'observation et de protection pour en faire une seule phase de prévention (figure 2).

Phase de prévention

À l'échelon individuel, les pratiques exemplaires en cybersécurité sont un moyen de prévention efficace contre les attaques. Les prestataires de soins de santé doivent être vigilants face à l'hameçonnage par courriel ou à tout autre comportement

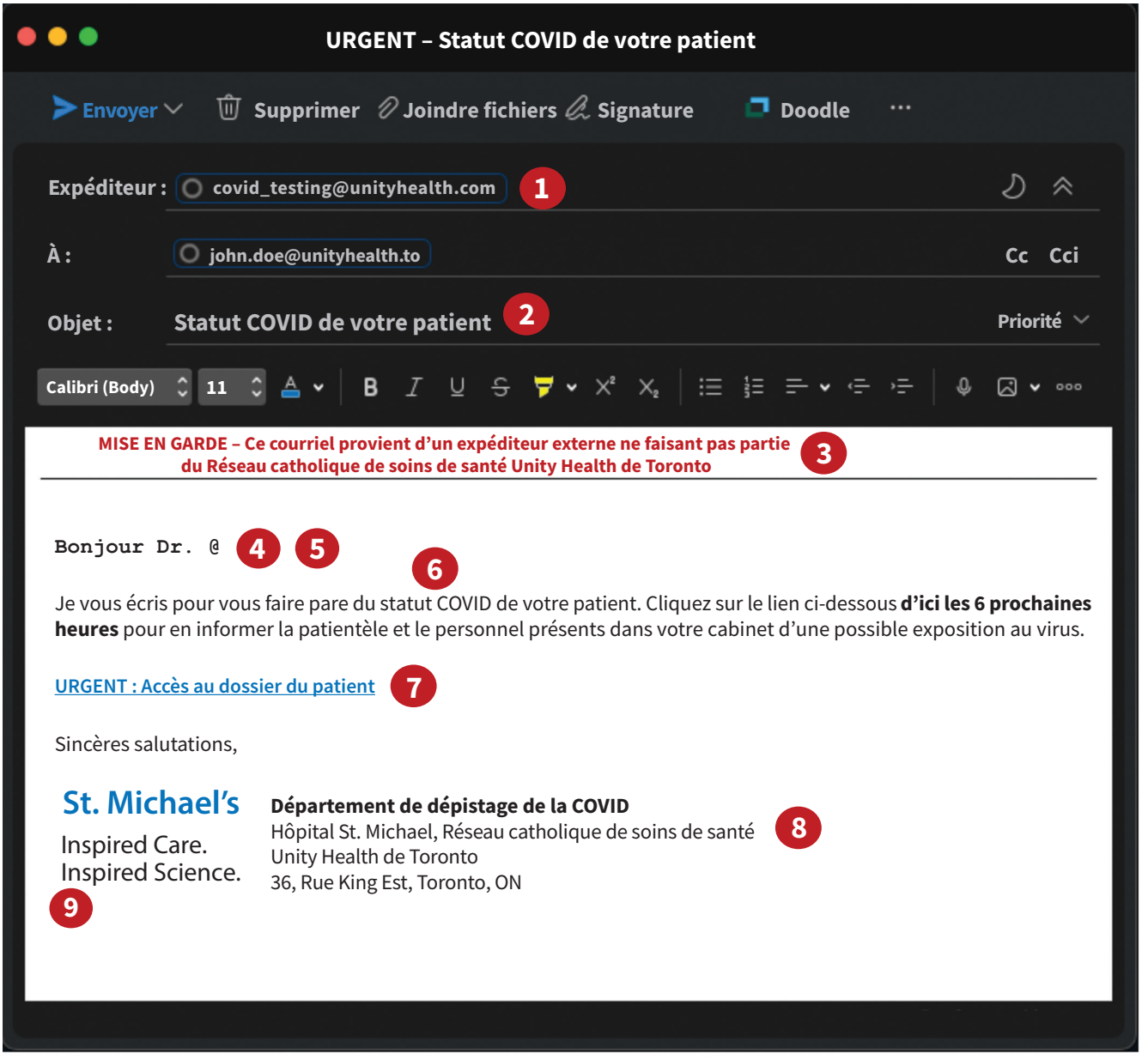

Figure 3 : Exemple annoté d'une attaque par hameçonnage potentielle.

suspect (figure 3). L'hameçonnage fait référence à des efforts ciblés et trompeurs visant à obtenir l'accès à un appareil ou au réseau d'une victime. Une fois cet accès obtenu, la personne cybercriminelle peut installer un logiciel malveillant pour exfiltrer ou crypter des données afin de demander une rançon. De ce fait, les prestataires de soins de santé devraient veiller à utiliser des mots de passe uniques et sécurisés (ils doivent notamment contenir au moins 8 caractères, une lettre, un chiffre et un caractère spécial) ainsi que l'authentification à 2 facteurs pour se connecter. Ils devraient aussi définir des questions de vérification et verrouiller automatiquement les appareils ayant accès à des RPS. En outre, les gestionnaires de mots de passe peuvent générer et stocker des mots de passe uniques et sécurisés pour chaque site Web et envoyer des notifications lorsque les informations des utilisatrices et utilisateurs sont compromises. De plus, les prestataires de soins de santé devraient éviter de se livrer à

des tâches nécessitant l'accès à des données confidentielles sans protection adéquate du réseau (p. ex., accéder aux DMÉ des patientes et patients sur un réseau Wi-Fi public), car les données peuvent ainsi être interceptées, ou des logiciels malveillants peuvent y être introduits dans le cadre d'attaques de type « homme du milieu ». Les logiciels devraient être tenus à jour, car les concepteurs de logiciels publient régulièrement des correctifs pour combler les failles de sécurité. Les organismes de santé sont connus pour leur maintien en place de systèmes archaïques (p. ex., Windows XP) bien après que le service d'assistance de sécurité soit devenu obsolète.

À l'échelon d'un hôpital ou d'un cabinet, un aspect essentiel de la prévention contre des cyberattaques consiste à réduire la surface d'attaque; c'est-à-dire, le nombre de points d'entrée que des intrus pourraient emprunter pour accéder aux systèmes d'information de santé. Ce point est particulièrement important dans les configurations où les membres du personnel peuvent utiliser leurs appareils privés et compte tenu du nombre croissant d'appareils IdO[20]. Les techniques pour réduire la surface d'attaque comprennent l'audit de tous les appareils sur le réseau, la vérification que les logiciels sur ces appareils (y compris les systèmes d'exploitation) sont à jour, l'installation de logiciels antivirus et antimaliciels, et la mise en place d'un pare-feu pour surveiller le trafic Internet sortant et entrant. Les cabinets peuvent également mettre en place un réseau privé virtuel (RPV aussi connu sous l'acronyme en anglais VPM pour virtual private network), qui crypte et dissimule le trafic en ligne, le rendant ainsi bien plus difficile à intercepter. Ces réseaux sont particulièrement utiles pour les prestataires de soins de santé qui souhaitent accéder aux RPS à partir d'environnements externes au réseau de leur organisme de santé, par exemple pour effectuer la tenue des dossiers médicaux à domicile. Si les prestataires de soins de santé travaillant dans des structures plus importantes bénéficient d'une approche normalisée, ceux qui exercent en cabinet privé devront s'en remettre à des fournisseurs tiers. Heureusement, de nombreux fournisseurs d'antivirus traditionnels proposent aujourd'hui des offres de services complètes. Des organismes comme l'Association médicale de l'Ontario apportent également un soutien professionnel, notamment en ce qui concerne les atteintes à la protection des données et la couverture de cyberassurance, afin d'aider les services médico-légaux, de relations publiques et juridiques. Les dépenses relatives à tous ces services devraient être perçues comme des dépenses administratives essentielles et, dans de nombreux pays, elles peuvent donner droit à des crédits d'impôt.

Phase de détection

Un comportement suspect peut être un signe de cyberattaque. Il peut s'agir, par exemple, d'une interdiction d'accès à des fichiers ou à des applications (DMÉ, clients de courriel, etc.), de la suppression de fichiers et de logiciels non reconnus ou de leur installation, de l'exécution automatique de programmes et de l'envoi de courriels non sollicités. Les attaques par rançongiciels sont souvent accompagnées de messages contextuels signalant aux utilisatrices et aux utilisateurs qu'ils sont victimes d'un piratage et donnent des instructions ainsi qu'une date limite pour payer la rançon. Les logiciels antivirus et antimaliciels peuvent aussi détecter des menaces lors d'analyses de routine. Enfin, les utilisatrices et utilisateurs internes d'un organisme peuvent signaler qu'ils ont suivi un lien dans un courriel d'hameçonnage ou qu'ils ont téléchargé des fichiers ou des applications inconnues.

Phase d'intervention

Dès qu'une cyberattaque est détectée, les prestataires de soins de santé devraient d'abord déconnecter d'Internet les appareils touchés et les éteindre. Une action rapide peut empêcher l'exfiltration de données, y compris des RPS provenant d'appareils ou du réseau d'un organisme de santé. Une fois cette mesure prise, les cabinets devraient mettre en œuvre leur plan d'intervention en cas de cyberattaque. Si l'accès aux systèmes informatisés tels que les DMÉ est perdu, le personnel devrait suivre des procédures de remplacement telles que l'utilisation de dossiers papier. En fonction de l'ampleur des perturbations du flux de travail et de la capacité des prestataires de soins de santé à maintenir un niveau de soins suffisant, des mesures d'urgence telles que l'annulation de consultations et le transfert de patientèle peuvent s'avérer nécessaires. Il est essentiel que les plans d'interventions ne relèvent pas de l'improvisation, mais qu'ils soient bien documentés et clairs et qu'ils fassent l'objet d'exercices bien planifiés[21]. Les prestataires de soins de santé devraient s'entraîner à réagir en cas de cyberattaque (code gris), comme ils le font en cas d'incendie (code rouge). Bien que la pression exercée sur les organismes de santé pour qu'ils paient les rançons en échange du déverrouillage et du décryptage des systèmes soit très forte, ils ne devraient pas le faire, car le rétablissement de l'accès n'est pas garanti, et le paiement de rançons risque d'encourager des attaques ultérieures.

L'Association canadienne de protection médicale (ACPM) souligne l'obligation des dépositaires d'aviser les personnes concernées par les atteintes à la vie privée (p. ex., la patientèle) ainsi que le commissaire à la protection de la vie privée et le ministère de la Santé[22]. Comme les attentes varient d'un système de santé à l'autre, l'ACPM recommande aux organismes et aux prestataires de soins de santé de communiquer avec ses services le plus tôt possible après la découverte d'une éventuelle atteinte à la vie privée. Ils devraient également en aviser les forces de l'ordre, en particulier en cas d'attaque par rançongiciel. D'ailleurs, la Gendarmerie royale du Canada teste actuellement un système national de signalement des incidents de cybercriminalité et de fraude[23]. Le Centre canadien pour la cybersécurité dispose aussi d'un système de signalement, mais celui-ci ne déclenche pas d'intervention immédiate de la part des services de police[24]. Dans le cadre de leur plan d'intervention en cas de cyberattaque, les prestataires de soins de santé travaillant dans des cabinets devraient consulter les autorités compétentes à l'avance pour s'assurer qu'ils comprennent bien les obligations en matière de signalement des brèches de sécurité et de notification des forces de l'ordre sur leur territoire.

Phase de redressement

Une fois que la menace immédiate d'une cyberattaque s'est dissipée, les prestataires de soins de santé et l'organisme au

sein duquel ils travaillent peuvent alors entrer en phase de redressement. Cette phase dépend fortement de l'existence ou non de systèmes d'information de santé qui permettent de restaurer les données à partir de copies de sauvegarde. Les prestataires de soins de santé travaillant dans des structures plus petites et des cabinets indépendants qui ne disposent pas d'experts en informatique devraient se renseigner sur la manière dont leurs fournisseurs protégeront leurs données et les aideront à les récupérer en cas d'attaque; il s'agit d'une mesure de diligence raisonnable à exercer lors de tout achat de ce type. Les organismes devraient aussi faire un bilan ciblé de leur intervention axé sur les possibilités d'amélioration et les mesures de bonification de leur posture future en matière de cybersécurité.

Les prestataires de soins de santé pourraient avoir l'impression que la mise en œuvre des mesures présentées ici ne fait qu'alourdir le fardeau que leur imposent les systèmes d'information de santé. Dans son célèbre essai paru dans le *New Yorker*, Atul Gawande a ironisé que les systèmes de DMÉ, « qui promettaient de me conférer une plus grande maîtrise de mon travail, [avaient] au contraire, renforcé la mainmise que mon travail exerce sur moi[25] ». La cybersécurité peut constituer une charge de travail supplémentaire, surtout pour les prestataires de soins de santé exerçant dans des cabinets de plus petite taille, puisqu'elle s'ajoute aux tâches liées à la documentation, à la saisie informatisée des ordonnances et au maintien des exigences en matière de permis d'exercice par le biais de modules électroniques obligatoires, autant de facteurs qui contribuent à l'épuisement professionnel[26,27]. La formation par simulation est également devenue monnaie courante en médecine, et certaines personnes peuvent se demander si des mesures supplémentaires s'avèrent nécessaires. Des mesures telles que l'authentification à 2 facteurs et les RPV ajoutent de la complexité au flux de travail. Cela dit, de petits changements dans les habitudes quotidiennes qui encouragent la mise en œuvre de pratiques exemplaires en cybersécurité sont nettement préférables au redressement opérationnel après une cyberattaque, tant sur le plan financier que sur celui de la confiance de la patientèle et de la communauté.

Quels sont les domaines émergents de la cybersécurité en matière de soins de santé?

Les nouvelles technologies nécessitent qu'on y consacre une attention particulière pour éviter que le risque de corruption ne devienne plus important à mesure que les fonctionnalités de ces technologies s'améliorent. Les prestataires de soins de santé qui utilisent une plateforme de soins virtuels doivent savoir que les solutions de vidéoconférence grand public (p. ex., Zoom ou FaceTime) ne répondent souvent pas aux exigences provinciales en matière de sécurité et de protection de la vie privée. Les prestataires de soins de santé devraient plutôt utiliser des outils intégrés à leur DMÉ ou des versions des solutions de vidéoconférence qui répondent explicitement aux normes du domaine de la santé, comme Zoom pour la santé[28]. Les autorités sanitaires provinciales fournissent des listes de solutions approuvées pour les soins virtuels[29]. Les dispositifs médicaux personnels, tels que les stimulateurs cardiaques, les pompes à insuline et les glucomètres, sont connectés à Internet pour assurer le monitorage des biomarqueurs et pour recevoir des mises à jour de logiciels. Les pirates informatiques ont démontré leur capacité à vider rapidement les batteries des appareils, à générer un excès de stimuli (rythme, bolus d'insuline, etc.) ou à en omettre lorsqu'ils sont cliniquement indiqués[30]. En 2019, Santé Canada a rappelé plusieurs modèles de pompes à insuline susceptibles d'être attaquées et a encouragé les patientes et patients à discuter avec leur médecin du remplacement de ces pompes par d'autres modèles[31]. Enfin, des outils d'apprentissage automatique sont en cours de développement et d'intégration dans les flux de travail en soins de santé[32]. Ces outils peuvent être vulnérables à des attaques ou à des modifications subtiles des données d'entrée, soigneusement conçues pour induire les algorithmes en erreur vers des résultats incorrects[33]. Par exemple, des pirates informatiques peuvent modifier les pixels d'une radiographie en ajoutant de très petites quantités de données parasites qui seraient imperceptibles aux humains, mais qui modifieraient les résultats du modèle (notamment un résultat bénin qui deviendrait pathologique, ou vice-versa). Dans ces nouveaux domaines, les prestataires de soins de santé et les organismes de santé devraient surveiller les rappels, maintenir leurs logiciels à jour et discuter des risques possibles avec leur patientèle.

Conclusion

La prévention des cyberattaques suppose de trouver des compromis entre le maintien de l'efficacité des flux de travail et la réduction des risques dans un contexte de menaces dont la fréquence, la gravité et la complexité ne cessent d'augmenter. À mesure que les politiques nationales et régionales évoluent, les organismes de santé et les prestataires de soins de santé travaillant dans des cabinets, indépendants ou non, doivent adopter une approche proactive pour améliorer leur position en matière de cybersécurité. Les méthodes de gestion des risques personnels et professionnels vont de pair, notamment l'utilisation d'outils et de pratiques exemplaires, l'adoption d'une attitude prudente et la mise en place d'un plan d'intervention en cas d'incident. Un peu de prévention vaut mieux qu'un téraoctet de guérison lorsqu'il s'agit de cybersécurité.

Références

1. *How Canada Compares: Results from the Commonwealth Fund's 2019 international Health Policy Survey of Primary Care Physicians*. Ottawa: Canadian Institute for Health Information; 2020:1-78. Accessible ici : https://www.cihi.ca/sites/default/files/document/cmwf-2019-accessible-report-en-web.pdf (consulté le 29 oct. 2023).
2. Cohen AB, Dorsey ER, Mathews SC, et al. A digital health industry cohort across the health continuum. *NPJ Digit Med* 2020;3:68.
3. HC3 intelligence briefing update dark web PHI marketplace: overall classification is unclassified. Washington (DC): The U.S. Department of Health & Human Services; 2019:1-13. Accessible ici : https://content.govdelivery.com/attachments/USDHSFACIR/2019/04/25/file_attachments/1199378/Dark%20Web%20primer.pdf (consulté le 29 oct. 2023).
4. The state of ransomware in healthcare 2021. Abingdon (UK): SOPHOS; 2021:1-16. Accessible ici : https://assets.sophos.com/X24WTUEQ/at/s49k3zrbsj8x9hwbm9nkhzxh/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf (consulté le 29 oct. 2023).

5. *The impact of ransomware on healthcare during COVID-19 and beyond*. Traverse City (MI): Ponemon Institute; 2021. Accessible ici : https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf (consulté le 29 oct. 2023). Connexion requise pour accéder au contenu.
6. Burke D. Hospitals 'overwhelmed' by cyberattacks fuelled by booming black market. *CBC News* le 2 juin 2020. Accessible ici : https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422 (consulté le 29 oct. 2023).
7. Alert: Cyber threats to Canadian health organizations. Canadian Centre for Cybersecurity; 2020. Accessible ici : https://www.cyber.gc.ca/en/alerts-advisories/cyber-threats-canadian-health-organizations (consulté le 29 oct. 2023).
8. Samarasekera U. Cyber risks to Ukrainian and other health systems. *Lancet Digit Health* 2022;4:e297-8.
9. Nigrin DJ. When 'hacktivists' target your hospital. *N Engl J Med* 2014;371:393-5.
10. Wilner AS, Luce H, Ouellet E, et al. From public health to cyber hygiene: cybersecurity and Canada's healthcare sector. *Int J* 2021;76:522-43.
11. Vinall F. Huge Australian health hack exposes abortion patients and others. *The Washington Post* le 10 nov. 2022, mis à jour le 11 nov. 2022; Accessible ici : https://www.washingtonpost.com/world/2022/11/10/australia-health-data-hack-abortion/ (consulté le 9 sept. 2023).
12. Schaffer A, Marks J, Knowles H. Planned parenthood Los Angeles says hack breached about 400,000 patients' information. *The Washington Post* le 1 déc. 2021; Accessible ici : https://www.washingtonpost.com/nation/2021/12/01/los-angeles-planned-parenthood-hack/ (consulté le 9 sept. 2023).
13. Taggart K. The hacker in the clinic: why physicians have become targets of ransomware attacks and what you should know. *The Medical Post*; 2019;32-4. Accessible ici : https://www.ontariomd.ca/articlesdocumentlibrary/hacker_in_the_clinic_med_post_oct_2019.pdf (consulté le 29 oct. 2023).
14. Landi H. UCSF pays hackers $1.1M to regain access to medical school servers. New York: Fierce Healthcare; 2020. Accessible ici : https://www.fiercehealthcare.com/tech/ucsf-pays-hackers-1-14m-to-regain-access-to-medical-school-servers (consulté le 29 oct. 2023).
15. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum* 2022;3:e224873.
16. Ahmad I, Cassell J, Corovic T, et al. Bill C-26: the increased importance of Canadian cybersecurity. Ottawa: Norton Rose Fulbright Insights; 2022. Accessible ici : https://www.nortonrosefulbright.com/en-ca/knowledge/publications/42944ded/bill-c26-the-increased-importance-of-canadian-cybersecurity (consulté le 29 oct. 2023).
17. Healthcare and public health sector: council charters membership. Arlington (VA): US Cybersecurity & Infrastructure Security Agency. Accessible ici : https://www.cisa.gov/healthcare-and-public-health-sector-council-charters-membership (consulté le 29 oct. 2023).
18. Jones P. How to deter cyber-attacks: TOH outlines its best practices. Thornhill (ON): Canadian Healthcare Technology; 2022. Accessible ici : https://www.canhealth.com/2022/09/01/how-to-deter-cyber-attacks-toh-outlines-its-best-practices/ (consulté le 29 oct. 2023).
19. Cybersecurity Framework (CSF). Gaithersburg (MD): National Institute of Standards and Technology; 2016, mis à jour le 15 août 2023. Accessible ici : https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters (consulté le 9 sept. 2023).
20. Alexandrou A, Chen L-C. Perceived security of BYOD devices in medical institutions. *Int J Med Inform* 2022;168:104882. doi : 10.1016/j.ijmedinf.2022.104882.
21. Report a cyber incident. Canadian Centre for Cyber Security; modifié le 21 févr. 2022. Accessible ici : https://www.cyber.gc.ca/en/incident-management (consulté le 9 sept. 2023).
22. Willing M, Dresen C, Gerlitz E, et al. Behavioral responses to a cyber attack in a hospital environment. *Sci Rep* 2021;11:19352.
23. Reporting a privacy breach: What are your responsibilities? Ottawa: Canadian Medical Protective Association; 2018, révisé septembre 2022. Accessible ici : https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2018/the-new-reality-of-reporting-a-privacy-breach (consulté le 29 oct. 2023).
24. New cybercrime and fraud reporting system. Ottawa: Royal Canadian Mounted Police; modifié le 23 sept. 2021. Accessible ici : https://www.rcmp-grc.gc.ca/en/new-cybercrime-and-fraud-reporting-system (consulté le 9 sept. 2023).
25. Gawande A. Why doctors hate their computers. *The New Yorker* le 5 nov. 2018; Accessible ici : https://www.newyorker.com/magazine/2018/11/12/why-doctors-hate-their-computers (consulté le 20 sept. 2023).
26. Sinsky C, Colligan L, Li L, et al. Allocation of physician time in ambulatory practice: a time and motion study in 4 specialties. *Ann Intern Med* 2016;165:753-60.
27. Hodzic-Santor B, Prakash V, Raudanskis A, et al. How many hours do internal medicine residents at University of Toronto spend onboarding at hospitals each year? A cross-sectional survey study. *medRxiv* 2022 June 14. doi : 10.1101/2022.06.10.22276103.
28. Appendix 2: Best practices security for Zoom virtual health visits. Vancouver: Provincial Health Services Authority; mis à jour le 2 juin 2020. Accessible ici : http://www.phsa.ca/health-professionals-site/Documents/Office%20of%20Virtual%20Health/Security%20best%20practices.pdf (consulté le 29 oct. 2023).
29. Verified solutions list for virtual visits. Toronto: Ontario Health. Accessible ici : https://www.ontariohealth.ca/system-planning/digital-standards/virtual-visits-verification/verified-solutions-list (consulté le 29 oct. 2023).
30. Baranchuk A, Refaat MM, Patton KK, et al.; American College of Cardiology's Electrophysiology Section Leadership. Cybersecurity for cardiac implantable electronic devices: What should you know? *J Am Coll Cardiol* 2018;71:1284-8.
31. Certain older Medtronic MiniMed insulin pumps may be vulnerable to cybersecurity risks [avis public]. Ottawa: Government of Canada, Health Canada, Communications and Public Affairs Branch; modifié le 29 juin 2019. Accessible ici : https://recalls-rappels.canada.ca/en/alert-recall/certain-older-medtronic-minimed-insulin-pumps-may-be-vulnerable-cybersecurity-risks (consulté le 29 oct. 2023).
32. Verma AA, Murray J, Greiner R, et al. Implementing machine learning in medicine. *CMAJ* 2021;193:E1351-7.
33. Finlayson SG, Bowers JD, Ito J, et al. Adversarial attacks on medical machine learning. *Science* 2019;363:1287-9.

Intérêts concurrents : Alun Ackery est directeur médical provincial de l'organisme de soins de santé CritiCall Ontario. Aucun autre intérêt concurrent n'a été déclaré.

Cet article a été révisé par des pairs.

Affiliations : Faculté de médecine Temerty) (Harish), Université de Toronto; Institut des politiques, de la gestion et de l'évaluation de la santé (Harish), École de santé publique Dalla Lana, Université de Toronto; Département de médecine d'urgence (Ackery, Mehta), Hôpital St. Michael, Réseau catholique de soins de santé Unity Health de Toronto, Toronto, Ont.; Département de médecine d'urgence (Grant), Faculté de médecine, Université de la Colombie-Britannique, Vancouver, C.-B.; Département de médecine interne générale (Jamieson), Hôpital St. Michael, Réseau catholique de soins de santé Unity Health de Toronto; Institut pour des solutions dans les systèmes de santé et les soins virtuels (Jamieson), Hôpital Women's College; Département de médecine d'urgence (Mehta), Hôpital général de North York, Toronto, Ont.

Collaborateurs : Tous les auteurs ont contribué à l'élaboration et à la conception du travail, ont rédigé l'ébauche du manuscrit et en ont révisé de façon critique le contenu intellectuel important; ils ont donné leur approbation finale pour la version destinée à être publiée et assument l'entière responsabilité de tous les aspects du travail.

Financement : Vinyas Harish est titulaire d'une bourse postdoctorale Banting des Instituts de recherche en santé du Canada, d'une bourse d'études supérieures du Canada au niveau du doctorat et d'une bourse de recherche doctorale de l'Institut Schwartz Reisman pour la technologie et la société.

Correspondance : Vinyas Harish, v.harish@mail.utoronto.ca