LIGNES DIRECTRICES À L'INTENTION DES MÉDECINS AU SUJET DES COMMUNICATIONS EN LIGNE AVEC LES PATIENTS

INTRODUCTION

La disponibilité et l'utilisation accrues d'Internet facilitent la communication en ligne entre médecins et patients lorsque le patient n'est pas présent physiquement au lieu de travail du médecin. Les communications en ligne peuvent être reliées directement à la prestation de soins aux patients ou servir à transmettre des renseignements plus généraux pour répondre à des besoins en administration, formation ou promotion de la santé. Les présentes lignes directrices portent principalement sur les deux moyens les plus courants de communication en ligne, soit le courrier électronique et les sites web de médecins.

Les communications électroniques offrent de nombreux avantages, mais elles exigent aussi des mesures de protection différentes des autres formes de communication comme le document sur papier, le téléphone et le télécopieur. Comme elles sont numérisées, les communications électroniques facilitent l'envoi, le stockage, le partage et la recherche rapides. Ces avantages inhérents posent toutefois aussi des défis en matière de protection de la vie privée et de confidentialité des renseignements. Le même renseignement peut être envoyé et stocké à de nombreux endroits, relié facilement à d'autres données et effectivement servir à des fins non prévues au moment de la collecte initiale.

Il faut dans la mesure du possible protéger la vie privée et la confidentialité des renseignements personnels à un niveau comparable à celui qu'on attend actuellement dans le cas du dossier papier. Les médecins doivent consulter le *Code de protection des renseignements personnels sur la santé* et le *Code de déontologie* de l'AMC, ainsi que les lois ou exigences particulières de leur province ou territoire, qui les guideront à cet égard.

Les présentes lignes directrices émanent de normes et de pratiques exemplaires qui ont émergé de l'utilisation de documents sur papier, du courrier, du téléphone et du télécopieur dans les bureaux de médecins. Elles tiennent compte aussi des défis uniques que posent la numérisation et la communication en ligne, ainsi que des possibilités qu'elles offrent d'ouvrir de nouveaux moyens de faciliter la prestation des soins et la diffusion de l'information. Le présent guide ne traite pas des communications des médecins avec d'autres prestateurs de soins de

santé, le gouvernement et d'autres tiers.

Compte tenu de l'éventail des façons possibles d'utiliser les communications en ligne, les médecins devraient établir un protocole qui décrit comment intégrer ces communications à leur pratique. Le protocole peut servir de base pour informer le personnel, les patients et d'autres interlocuteurs au sujet des limites et des règles associées à l'utilisation de l'information transmise en ligne.

Le protocole devrait aborder tous les aspects suivants :

a. Raisons pour lesquelles le bureau utilise les communications en ligne.
b. Relations patient–médecin en ligne (à distance).
c. Réponse aux demandes de renseignements des patients – gestion des attentes.
d. Conditions d'utilisation des communications en ligne par les patients.
e. Triage des communications.
f. Accès aux demandes de renseignements des patients.
g. Conservation, format et organisation des communications.
h. Type et qualité de l'information fournie aux patients.
i. Protection de la vie privée, confidentialité et sécurité.
j. Dispositions et exigences particulières selon les régions.

Nous abordons chacun de ces sujets plus en détail ci-dessous. Il faudra en outre traiter de questions techniques précises et nous présentons une liste de contrôle et un tour d'horizon à cette fin (Annexe A).

LIGNES DIRECTRICES

a. Raisons pour lesquelles le bureau utilise les communications en ligne

Voici un éventail d'utilisations possibles des communications en ligne. Les médecins doivent s'assurer qu'ils communiquent uniquement pour les raisons précises adoptées par leur pratique.

Administration

- Prise de rendez-vous (y compris report et annulation).
- Paiement en ligne de services non assurés ou assurés autrement.
- Communication de renseignements sur la façon de se rendre au lieu de pratique et à d'autres établissements.
- Communication des politiques et des protocoles de la pratique (p. ex., politiques sur la protection de la vie privée, lignes directrices sur la facturation de services non assurés, protocoles relatifs à des demandes de tiers).

Information et promotion de la santé

- Fournir des documents et des ressources électroniques de formation et de promotion de la santé en général.
- Fournir des liens vers des sites web d'information et de promotion de la santé.
- Intégrer les messages de promotion de la santé.
- Fournir des liens vers des outils d'aide et d'autoévaluation en ligne.
- Conseiller des patients au sujet de sites web sur la santé.
- Bulletins et avertissements.
- Services d'appui communautaires.

Soin des patients

- Recevoir des demandes de renouvellement d'ordonnances de patients.
- Clarifier ou répéter des instructions.
- Recevoir des questions de suivi des patients et y répondre.
- Fournir des instructions et des suivis après une intervention.
- Donner des avis ou des rappels au sujet d'examens et d'interventions de routine.
- Assurer de la surveillance.
- Communiquer des résultats d'examen (lorsqu'il est acceptable de le faire).
- Donner des conseils au sujet de problèmes dont on a déjà discuté.
- Donner des conseils au sujet de nouveaux problèmes.

b. Relation patient–médecin en ligne (à distance)

Dans toute communication en ligne (ou à distance), les médecins doivent se guider sur leurs obligations professionnelles envers le patient, qui demeureront tout aussi rigoureuses dans les échanges en ligne.

Patients actuels du médecin : La plupart des communications en ligne sont échangées entre des médecins et des patients actuels. Les médecins doivent établir un moyen d'assurer qu'ils communiquent bien avec des patients inscrits et dans le contexte d'une relation patient–médecin.

Non-patients : Les médecins doivent éviter de sembler dispenser des conseils médicaux à des non-patients et d'établir par inadvertance une relation patient–médecin par l'échange d'information. À cette fin, on peut recourir à des moyens comme des avis affichés sur des sites web ouverts qui décrivent à qui s'adresse l'information contenue sur le site, des sites web fermés (protégés par mot de passe) et une réponse automatisée et normalisée aux non-patients.

Patients éventuels : Dans le cas de patients référés et de nouveaux patients, par exemple, les médecins voudront peut-être établir une communication préliminaire par voie électronique, notamment pour :

- donner un rendez-vous;
- réunir de l'information préliminaire, comme les renseignements nécessaires pour communiquer avec le patient et ses antécédents médicaux de base;
- fournir de l'information de base sur la visite au bureau.

Dans de tels cas, et même si l'on n'a pas établi de relation patient–médecin en personne, il est recommandé de veiller à ce que le patient accepte les conditions et les limites des communications en ligne. Si l'on fournit ainsi des renseignements médicaux préliminaires, il faut aussi préciser clairement que les renseignements seront revus seulement lorsque le patient se présentera à son premier rendez-vous. Il faut aussi lui donner des instructions au sujet d'autres moyens de se faire traiter s'il en a besoin avant le premier rendez-vous.

Patients virtuels[1] *:* Il y a actuellement tout un éventail de lignes directrices qui semblent décourager ou interdire la relation patient–médecin purement en ligne ou virtuelle. On insiste en général sur l'importance des contacts en personne et sur l'utilisation des communications électroniques uniquement comme moyen de suivi, de clarification et de surveillance, etc., dans le contexte d'une relation qui existe déjà. La technologie de la télésanté permet toutefois aux cliniciens d'établir des protocoles de pratique et de dispenser des soins à distance. Le domaine est en émergence et à mesure que la technologie deviendra plus sophistiquée et ses utilisateurs, plus avertis, on pourra très bien alors remettre en question l'hésitation actuelle à l'utiliser. La question se posera sans doute particulièrement lorsque l'accès physique à un médecin est sérieusement limité ou inexistant (p. ex., en région éloignée ou en contexte d'urgence) et qu'il est démontré que les avantages d'une relation virtuelle l'emportent sur l'absence totale d'accès.

c. Réponse aux demandes de renseignements des patients – gestion des attentes

Il se peut que la rapidité avec laquelle les patients s'attendent à ce que le médecin ou son bureau réponde à leurs demandes de renseignements en ligne ne soit pas réaliste. Les médecins doivent déterminer comment gérer ces attentes et communiquer clairement aux patients le protocole de leur bureau au sujet des temps de réponse. Les mécanismes ci-dessous peuvent aider à clarifier et à faire connaître les attentes, ainsi qu'à gérer en général la circulation des messages électroniques.

- Établir des temps de réponse raisonnables – des demandes de renseignements différentes peuvent justifier des temps de réponse différents. Dans les temps de réponse, il faut tenir compte des périodes de fermeture de la

1 On a utilisé cette expression pour décrire un patient qu'un médecin n'a jamais vu en personne mais qui entretient néanmoins une relation patient–médecin avec le médecin.

pratique (fins de semaine, vacances, jours fériés).
- Accuser automatiquement réception des communications et indiquer le protocole que l'on suivra pour y répondre.
- Fournir des instructions sur l'accès à des solutions de repli en cas d'urgence.
- Encourager ou exiger l'ajout d'une rubrique sujet.
- Trier les messages en fonction de la rubrique sujet et établir une procédure à suivre pour répondre à chaque type de message.
- Limiter le temps nécessaire pour lire les communications de patients : répondre en encourageant ou en obligeant les patients à limiter la longueur de leur texte, en restreignant les communications à des questions simples ou uniques et en encourageant les patients ou en les obligeant à se rendre au bureau pour traiter de questions complexes.
- Utiliser des modèles pour encourager ou imposer la communication normalisée (ce qui peut avoir des avantages sur les plans du stockage et de l'établissement de liens).
- Annoncer les temps de réponse (sur le site web du médecin, dans une réponse automatisée, dans les instructions initiales aux patients, dans une entente avec les patients). Inclure des instructions sur les urgences ou des consignes à suivre si l'on ne reçoit pas de réponse dans le délai indiqué.

d. Conditions d'utilisation des communications en ligne par les patients

Il est souhaitable d'assurer que les patients connaissent la limite des communications en ligne et les règles qui les régissent et, lorsque c'est possible, qu'ils consentent officiellement à se conformer à ces conditions. On pourrait obtenir leur consentement écrit en ligne en leur demandant de cliquer sur le consentement approprié, à condition que le médecin ait un moyen d'authentifier l'identité de la personne qui donne son consentement. Il faudrait prévoir la possibilité pour les patients qui ont des questions d'en discuter avec leur médecin avant de donner leur consentement.

Les conditions d'utilisation pourraient inclure les suivantes :

- Reconnaissance des utilisations permises des communications en ligne et consentement à les utiliser seulement à ces fins.
- Connaissance du fait que les membres du personnel du bureau ont accès aux communications en ligne et consentement pertinent à cet égard.
- Reconnaissance de l'existence d'autres sources de communication dans des circonstances précises, comme en cas d'urgence ou lorsque l'on ne reçoit pas de réponse.
- Consentement à se conformer au protocole établi à l'égard de questions comme les rubriques par sujet, la longueur du texte et l'utilisation de modèles.
- Vérification de l'adresse électronique du patient et entente au sujet de la responsabilité du patient d'empêcher l'accès non autorisé à son propre système.
- Reconnaissance de la nature non protégée des communications en ligne.
- Reconnaissance du fait que la communication pourrait être versée au dossier du patient.
- Consentement à s'abstenir d'utiliser un langage injurieux.
- Consentement à s'abstenir d'utiliser les communications en ligne pour des raisons non essentielles ou commerciales.
- Reconnaissance du fait que l'inobservation des conditions d'utilisation peut entraîner le retrait de l'autorisation d'utiliser la communication en ligne.
- Consentement à recevoir des communications périodiques du médecin en ce qui a trait à des questions comme des rappels de médicaments, des avertissements, la promotion de la santé et la prévention des maladies.
- Consentement à payer des frais d'utilisation de la capacité en ligne (lorsque la communication en ligne n'est pas un service assuré).

e. Triage des communications

Afin de permettre l'administration efficace des communications des patients, il faut les

encourager ou les obliger à utiliser des rubriques sujets normalisées pour décrire le type de demandes de renseignements. Si la communication se fait par le biais du site web du médecin, un menu déroulant serait utile à cette fin. Si la communication se fait par courrier électronique, on peut utiliser une réponse automatisée ou manuelle pour répondre aux communications qui ne sont pas conformes au format normalisé. La réponse devrait inclure la liste des rubriques sujets normalisés. Il faut indiquer aux patients que s'ils ne reçoivent pas de réponse à leur communication, ils doivent supposer que le message électronique n'a pas été reçu.

Afin de distinguer les communications destinées aux médecins de celles qui s'adressent aux membres du personnel du bureau, on peut utiliser des comptes de courrier électronique distincts ou des options en ligne et les patients doivent comprendre clairement quand ils doivent utiliser quelle adresse. Il faut établir une procédure claire d'acheminement des communications à l'intérieur du bureau afin que la personne compétente réponde à tous les messages dans un délai approprié.

Les médecins devront se pencher sur le problème des communications non désirées ou non sollicitées (pourriels). Il existe toutes sortes de produits pour filtrer les messages indésirés. Il faut toutefois veiller à assurer que les messages légitimes ne sont pas effacés par inadvertance ou que l'on ne leur bloque pas l'accès au système du médecin.

f. Accès aux demandes de renseignements des patients

Contrairement aux conversations privées que les patients ont avec les médecins au bureau, les conversations en ligne sont ouvertes à des tiers. Un protocole devrait traiter des questions suivantes.

- Le médecin sera-t-il la seule personne à recevoir les demandes de renseignements du patient ou le protocole est-il ouvert aux autres médecins du bureau (p. ex., pour faciliter les périodes de garde)?
- Si les membres du personnel du bureau sont le premier point de contact, il faut indiquer comment adresser les messages destinés aux médecins, les acheminer, les stocker et finalement y répondre.
- Comme il se peut que les patients s'attendent à communiquer directement avec le médecin et seulement avec lui dans le contexte d'un «espace privé», il faut leur indiquer dans quelle mesure d'autres personnes ont accès à ces communication et préciser que la nature même de la communication (numérisée, écrite et entièrement enregistrée) la rend plus vulnérable à l'accès par des tiers.

g. Conservation, format et organisation des communications

Toutes les communications échangées avec les patients entraîneront la création d'un certain nombre d'enregistrements, y compris des dossiers à la fois électroniques et sur papier détenus autant par les médecins que par le patient. Pour déterminer ce qu'il faut conserver et dans quelle forme le faire, les médecins voudront sans doute tenir compte du fait que le patient garde un dossier et de la nécessité d'en conserver un double afin de répondre aux patients ou à des tiers au sujet d'une question précise se rattachant au dossier. Les médecins devraient se demander s'ils doivent abréger des parties pertinentes de la communication ou simplement joindre la communication au complet au dossier du patient sous forme électronique ou sur papier.

En élaborant des procédures sur la conservation et l'organisation des communications électroniques, les médecins devraient consulter d'abord les exigences réglementaires de leur province ou territoire. À mesure que les communications électroniques et les dossiers électroniques de patients se répandent, il est probable que l'on mettra aussi à jour ces exigences. C'est pourquoi une étude périodique des règlements en vigueur est aussi souhaitable.

Il faudrait réfléchir à l'organisation des dossiers électroniques et sur papier, ainsi qu'à leur interdépendance. Il faudrait aussi réfléchir à la façon d'intégrer les communications

électroniques au dossier électronique lorsque c'est pertinent.

h. Type et qualité de l'information fournie aux patients

Les communications en ligne offrent un moyen de diffuser aux patients, par le site web d'un médecin ou par courrier électronique, des renseignements précieux pour des fins d'éducation, de promotion de la santé et de clarification. En choisissant le type d'information (ou le lien web) à fournir, le médecin doit :

- assurer que le patient sait que l'information sert à des fins générales seulement et qu'il ne faut pas la percevoir comme un conseil médical dispensé par les médecins; il faut encourager les patients à discuter de leurs problèmes précis avec leur médecin;
- fournir au patient seulement des documents provenant de sources crédibles (ou des liens vers celles-ci), comme des journaux critiqués par des pairs et des sociétés de spécialité;
- assurer que l'information est à jour; les médecins peuvent envisager des moyens électroniques à cet égard (p. ex., élimination automatique des documents périmés);
- assurer qu'ils respectent les règles régissant le droit d'auteur et ne diffusent pas de renseignements sans le consentement de leurs auteurs ou propriétaires;
- préciser clairement, lorsqu'ils fournissent des liens web, que l'utilisateur quitte leur site web.

i. Protection de la vie privée, confidentialité et sécurité

Nature délicate des renseignements transmis et importance des mesures de sécurité en place : Le type de renseignements transmis par Internet peut varier des données relativement bénignes (p. ex., heure d'un rendez-vous) à celles qui sont très délicates (p. ex., résultats d'examen ou diagnostic qui peut avoir des conséquences défavorables). En règle générale, il faut transmettre des renseignements de nature délicate par Internet *seulement* s'il existe des mécanismes de sécurité suffisants pour assurer la protection de la vie privée et de la confidentialité des renseignements. Il faut éviter de transmettre des résultats d'examen défavorables : il faut en général présenter ceux-ci pendant un contact en personne avec le patient afin de lui permettre d'en discuter directement avec le médecin.

La nature délicate des renseignements est liée jusqu'à un certain point à la connaissance subjective, au jugement et à l'expression de chaque patient et il ne faut pas supposer que tous les patients ont la même opinion de ce qui constitue un renseignement de nature délicate. Il faut préciser aux patients le type de communication que le médecin fera par courrier électronique et les mesures de sécurité qu'il a mises en place. Il faut aussi permettre aux patients de préciser leurs préférences en ce qui a trait à l'échange d'information par courrier électronique et leur dire s'il est possible d'en tenir compte.

Moyens de transmission : La communication électronique se fait en général par Internet, par réseau local ou (de plus en plus) par des moyens sans fil[2] et peut être plus ou moins sécuritaire : tout dépend de la façon dont la communication est protégée contre la consultation indue. Il faut en général dissuader les patients de recevoir des communications électroniques à des endroits où des tiers pourraient en garder un enregistrement ou y avoir accès (au travail, par exemple).

Il faut informer les patients au sujet des pratiques du bureau et leur recommander de prendre les précautions qu'ils jugent nécessaires pour protéger la confidentialité de leurs dossiers sur leur système à domicile.

Au bureau du médecin, il faut protéger la vie privée et la confidentialité des renseignements électroniques au même niveau que celui

2 Il faut accorder une attention particulière à la sécurité de l'information lorsqu'on utilise des dispositifs sans fil (l'Annexe A contient plus de détails).

actuellement prévu ou obligatoire[3] pour les communications sur papier, par téléphone ou télécopieur. Afin d'assurer un niveau de sécurité suffisant, il faut envisager le chiffrage ou la protection par mot de passe, ainsi que la possibilité d'utiliser des services protégés pour afficher et extraire des communications.

Il faut s'assurer que le fournisseur de services choisi peut protéger adéquatement la confidentialité des renseignements sur le patient conformément aux attentes du médecin, aux lois du Canada et aux exigences des organismes de réglementation des médecins. Il faut aussi tenir compte de l'endroit où se trouve le fournisseur de services afin de s'assurer que toutes les protections prévues dans les lois canadiennes, provinciales ou territoriales s'appliquent. (L'Annexe A fournit d'autres détails sur ces questions techniques.)

Interexploitabilité, sécurité et caractère pratique : Si l'on veut utiliser le courrier électronique pour transmettre divers renseignements, il faudra veiller à ce qu'il soit possible de transmettre des renseignements de nature délicate (ce qui inclut les renseignements médicaux) en toute sécurité et, de préférence, conformément aux normes reconnues et acceptées régissant la collecte, l'utilisation et la divulgation de renseignements personnels. La tâche n'est pas facile. Même si un médecin peut mettre en œuvre un moyen protégé de communiquer avec ses patients, il se peut que le même moyen ne soit pas une façon pratique de communiquer avec d'autres prestateurs de soins de santé. Un médecin pourrait, par exemple, utiliser le chiffrage, ce qui l'obligera à fournir à chaque destinataire une clé pour lui donner accès à l'information. Dans le cas des échanges entre médecins et patients, cette solution peut être pratique, mais si on l'utilise entre prestateurs, elle pourrait obliger chacun d'entre eux à connaître et utiliser de multiples clés.

Vérification et authentification : Il faut faire preuve de prudence pour réduire au minimum la possibilité qu'un message électronique soit envoyé à la mauvaise adresse ou reçu par mauvais destinataire. Il y a divers moyens à utiliser à cette fin, y compris les suivants :

- Techniques d'authentification[4].
- Extraction d'adresses électroniques d'un carnet d'adresses électroniques où elles ont été entrées avec soin (semblable à une fonction préprogrammée sur le télécopieur).
- Recommander vivement aux patients de recevoir leurs messages électroniques à une adresse électronique protégée par mot de passe et accessible seulement par eux (p. ex., pas au travail).
- Procédures générales consistant à vérifier deux fois l'adresse avant de l'envoyer.
- Énoncé ajouté à chaque message électronique prévoyant des circonstances où le mauvais destinataire reçoit un message électronique
- Ne pas envoyer de messages électroniques à de multiples destinataires (diffusion générale) et ne pas permettre à chaque destinataire de voir qui d'autre a reçu le message (violation de la confidentialité).

Mesures de protection physique : Le système informatique utilisé par le médecin doit être protégé par des moyens matériels visant à protéger l'intégrité des données stockées et à réduire le risque de modification, de perte, de consultation, de divulgation ou de vol. Ces moyens comprennent les suivants :

- Placer le système informatique dans un espace protégé.
- Obliger à utiliser des mots de passe et les changer régulièrement.
- Assurer que les écrans d'ordinateur du bureau sont positionnés de façon à empêcher les personnes non autorisées de les lire[5].
- Installer un logiciel antivirus fiable et le tenir à jour.

3 Dans certaines administrations, les organismes de réglementation imposent des exigences précises en ce qui a trait aux communications par téléphone, télécopieur ou courrier électronique.

4 À noter que ce moyen peut être difficile à mettre en œuvre.

5 À cette fin, on peut aussi installer un filtre de confidentialité sur l'écran de l'ordinateur.

- Installer un coupe-feu[6].
- Effectuer régulièrement des copies de sauvegarde du système et, idéalement, les garder à un endroit protégé ailleurs que sur les lieux de la pratique.
- S'assurer que le disque rigide des vieux systèmes informatiques que l'on jette est convenablement détruit.
- Lorsqu'on jette des donnée stockées sur d'autres supports (p. ex., CDROM, ANP), il faut veiller à ce que tous les éléments de données soient complètement effacés.

Mise à jour ou création de la politique du bureau sur la protection de la vie privée : Il faut mettre à jour la politique du bureau sur la protection de la vie privée afin d'y inclure l'utilisation du courrier électronique et les mesures de protection en place[7].

j. Dispositions et exigences particulières selon les régions

Les médecins du Canada sont en général autorisés à pratiquer la médecine par une province ou un territoire et ne peuvent pratiquer en dehors de l'administration où ils sont autorisés à le faire. Lorsqu'ils utilisent des communications électroniques, ils devraient éviter de pratiquer la médecine en dehors de l'administration qui les autorise à le faire. Les énoncés ajoutés au courrier électronique et sur le site web d'un médecin peuvent clarifier son intention à cet égard et réduire aussi sa responsabilité civile face à ceux qui affirment s'être fiés sur l'information fournie par le médecin

6 Combinaison de matériel et de logiciels conçus pour contrôler la circulation de l'information entre des ordinateurs et Internet (source : *Digital defense: what you should know about protecting your company's asset* by Thomas J. Parenty, Harvard Business School Press, 2003).

7 On recommande aux médecins d'avoir une politique du bureau sur la protection de la vie privée à laquelle les patients ont accès.

Annexe A – Liste de contrôle en matière de sécurité[8]

La sécurité de l'information peut exiger des connaissances spécialisées, mais l'approche ne diffère pas beaucoup de la façon d'assurer la sécurité physique de votre bureau. Par exemple, lorsque vous avez installé les portes et les serrures de vos locaux, vous avez probablement tenu compte des facteurs suivants :

- Utilisabilité.
- Fonctionnalité.
- Sécurité.
- Fiabilité.
- Coût.
- Entretien.

C'est la même chose dans le cas de vos systèmes et de votre accès réseau. Pour choisir et installer des logiciels d'application générale et des mesures spécifiques de sécurité de l'information, il faut tenir compte des mêmes facteurs et coûts. Les mesures que vous prenez pour assurer la sécurité matérielle de votre bureau semblent probablement naturelles. Il s'agit toutefois d'une réponse apprise à des menaces et à des vulnérabilités connues. Les portes verrouillées et les classeurs protégés sont des mesures de sécurité que nous tenons pour acquises. Il faut agir de la même façon pour protéger nos réseaux et nos systèmes d'information.

Comme dans le cas d'autres achats, une bonne sécurité de l'information exige à la fois un effort initial et des vérifications continues. Vous devez faire votre recherche avant d'acheter un logiciel de sécurité, du matériel ou des services d'entretien. Même si vous devez vous attendre à ce que la technologie fonctionne bien, il faut quand même procéder aux vérifications nécessaires pour vous assurer que c'est bien le cas. Il faut déterminer les caractéristiques appropriées et les adapter pour pouvoir travailler avec les ordinateurs, logiciels et connexions réseau que vous utilisez actuellement. On crée de nombreuses vulnérabilités sur le plan de la sécurité lorsqu'on installe une nouvelle application et qu'on laisse simplement tous les réglages implicites en place, ce qui les rend beaucoup plus faciles à manipuler pour des utilisateurs non autorisés.

Cela peut sembler compliqué ou intimidant au départ, mais avec le temps, vos interventions deviendront tellement connues et automatiques qu'elles constitueront une «culture de la sécurité». Personne ne s'attend à ce qu'un médecin revoie le code d'un logiciel ou comprenne les rouages complexes du matériel. Vous pouvez et devez toutefois lire les renseignements pertinents, poser des questions pertinentes et vous faire expliquer ce qui ne semble pas clair. En prenant l'initiative et en montrant que la sécurité est importante pour votre bureau, vous pouvez faire beaucoup pour assurer que vos systèmes d'information évoluent en demeurant protégés. Dans certains cas, par exemple lorsqu'on apporte des modifications importantes à vos systèmes d'information, vous aurez peut-être besoin de l'aide d'experts pour la configuration initiale et la mise en service du système. Il est essentiel de demander continuellement aux experts ce qu'ils font et pourquoi ils le font et de vous convaincre que les choix que vous avez faits reflètent vos besoins administratifs et améliorent la sécurité de l'information de votre entreprise.

Même avec une expertise et des ressources limitées, il y a beaucoup de choses que vous pouvez faire pour aider à protéger votre système TI et l'accès à votre réseau. Réfléchissez aux questions qui suivent. Prenez-vous ces mesures?

- Votre ordinateur est-il doté d'un coupe-feu si vous avez un accès Internet (et en particulier un accès à large bande)?
- Avez-vous un logiciel de détection et de destruction des virus transmis par courrier électronique ou dans des documents?
- La sécurité est-elle un critère important lorsque vous choisissez un logiciel ou des fournisseurs de services?

8 Le contenu de cette annexe représente une version condensée d'un document de l'OCDE intitulé «Information Security Issues and Resources for Small and Entrepreneurial Companies – A Business Companion to the 2002 OECD Guidelines for Security of Networks and Information Systems» produit par la «Chambre de commerce internationale».

- Comprenez-vous les fonctions de sécurité du logiciel et du matériel que vous avez déjà?
- Quelqu'un à votre bureau a-t-il déjà suivi un cours d'informatique pour se familiariser davantage avec ces fonctions?
- Si vous avez les ressources voulues et qu'il soit approprié de le faire, avez-vous consulté un expert local au sujet de la configuration et du déploiement de votre système TI?
- Avez-vous vérifié s'il y a des ressources ou de l'information du gouvernement, d'une association commerciale ou d'une chambre de commerce locale dans le domaine de la sécurité informatique?
- Avez-vous pris des mesures pour protéger physiquement vos ordinateurs, et en particulier les ordinateurs et les appareils portatifs?
- Faites-vous régulièrement des copies de sauvegarde de vos données hors site? Vérifiez-vous vos copies de sauvegarde?
- Obligez-vous vos employés à utiliser des mots de passe?
- Les mots de passe utilisés contiennent-ils à la fois des lettres et des chiffres?
- Les mots de passe sont-ils gardés de façon protégée (non consignés par écrit ou partagés, p. ex.) et changés au moins une fois aux trois mois?
- Essayez-vous de donner à vos employés une formation sur la sécurité de l'information?

Voici une liste de mesures que vous pouvez prendre pour améliorer le niveau de sécurité des aspects liés à la technologie de l'information à votre bureau.

Sécurité physique

- Installez des serrures appropriées ou d'autres moyens de contrôle physique sur les portes et fenêtres des pièces où vous gardez vos ordinateurs.
- Protégez physiquement les ordinateurs portatifs lorsqu'ils sont sans surveillance (p. ex., en les déposant dans un tiroir verrouillé le soir).
- Assurez-vous que vous contrôlez et protégez tous les supports amovibles, comme les disques rigides amovibles, les disques compacts, les disquettes et les lecteurs USB, fixés à vos éléments d'actif critiques pour votre entreprise.
- Assurez-vous de détruire ou de supprimer toute information critique pour l'entreprise de supports comme des disques compacts et des disquettes avant d'en disposer. N'oubliez pas que souvent, il ne suffit pas d'effacer un fichier pour le rendre impossible à récupérer.
- Assurez-vous que tout renseignement crucial pour votre entreprise est supprimé des disques rigides de tout ordinateur usagé avant d'en disposer.
- Gardez des copies de sauvegarde de vos renseignements critiques pour votre entreprise hors site ou dans un contenant à l'épreuve du feu et de l'eau.

Contrôle de l'accès

- Utilisez des mots de passe uniques qui ne sont pas évidents (pas de date de naissance ou de renseignement facile à trouver ou à deviner) et changez-les régulièrement, de préférence aux trois mois.
- Utilisez des mots de passe d'au moins six caractères et contenant des majuscules et des minuscules, des chiffres et des symboles.
- N'écrivez pas votre mot de passe et ne le révélez jamais à quiconque. Si vous devez le faire, assurez-vous de le changer le plus tôt possible – même si vous faites vraiment la confiance à la personne à qui vous l'avez dévoilé!

Technologie de la sécurité

- Il faut installer un logiciel antivirus sur tous les ordinateurs utilisés à votre bureau et mettre à jour les définitions de virus au moins une fois par semaine (beaucoup de fournisseurs offrent une mise à jour par un seul clic).
- Il faut filtrer, au moyen d'un logiciel antivirus, tous les messages d'arrivée et de départ, ainsi que les disquettes ou disques compacts utilisés, même s'ils proviennent d'une source «digne de confiance». Il faut

soumettre les ordinateurs à un dépistage de virus au moins une fois par mois et de préférence tous les jours.

- Si vos ordinateurs sont branchés à Internet, et surtout si vous avez une connexion à large bande, il faut utiliser un logiciel qui aide à empêcher du code malicieux de pénétrer dans votre ordinateur et de compromettre peut-être la confidentialité de votre réseau, son intégrité et sa disponibilité. Ce logiciel aide aussi à empêcher qu'on utilise votre système pour en attaquer d'autres à votre insu. Des logiciels coupe-feu destinés à des non-professionnels sont facilement disponibles à un coût raisonnable. Votre système d'exploitation, logiciel antivirus ou fournisseur de services Internet peuvent aussi offrir un coupe-feu. Des revues spécialisées populaires et destinées aux consommateurs comparent des fonctions et des caractéristiques coupe-feu de produits bien connus et sont donc une bonne source d'information. Il existe des partagiciels coupe-feu gratuits, mais il faut habituellement posséder des connaissances d'expert pour bien les utiliser.
- Mises à jour du système et rustines : Des logiciels complexes contiendront toujours des faiblesses. Des pirates criminels peuvent essayer d'exploiter ces faiblesses et le seul moyen de vous protéger consiste à appliquer des «rustines» (*patches*) fournies par les vendeurs. Réglez si possible votre système pour qu'il procède automatiquement à des mises jour en téléchargeant les rustines disponibles ou assurez-vous au moins de les appliquer aussi rapidement que possible.
- Si votre bureau est doté d'un petit réseau interne branché à Internet, il faut envisager d'installer une boîte «tout inclus» contenant un coupe-feu, un programme antivirus et un système de détection des intrusions, ce qui vous simplifiera énormément l'utilisation et la maintenance de la technologie de la sécurité Internet essentielle.

Personnel

- Donnez à tous les nouveaux employés une introduction simple à la sécurité de l'information et assurez-vous qu'ils lisent et comprennent votre politique en la matière. Assurez-vous qu'ils savent où trouver les détails des normes sur la sécurité de l'information et des procédures pertinentes à leurs rôles et responsabilités.
- Assurez-vous que les employés ont accès seulement aux éléments d'information dont ils ont besoin pour faire leur travail. S'ils changent de poste, assurez-vous qu'ils n'ont plus accès aux éléments d'information dont ils avaient besoin pour faire leur ancien travail. Lorsque vous congédiez des employés, assurez-vous qu'ils n'apportent pas avec eux d'information critique pour votre entreprise.
- Assurez-vous qu'aucun ancien employé ne conserve de droits d'accès à vos systèmes.
- Assurez-vous que vos employés connaissent les moyens courants que l'on peut prendre pour compromettre votre système. Ces moyens comprennent des messages électroniques contenant des virus et des trucs de «d'ingénierie sociale» utilisés par les pirates pour exploiter l'aide des employés afin de réunir de l'information qui leur donne accès à votre système. Un pirate qui utilise le téléphone pour se faire passer pour un ingénieur en maintenance de systèmes ou qui prétend être un nouvel employé : voilà un exemple «d'ingénierie sociale»

Incident de sécurité et réponse

- On entend par incident de sécurité tout événement qui peut endommager ou compromettre la confidentialité, l'intégrité ou la disponibilité de l'information ou des systèmes critiques pour votre entreprise.
- Les faiblesses de vos logiciels constituent une importante source possible d'incidents de sécurité. Il faut y appliquer une «rustine» le plus tôt possible après que le fournisseur de logiciels a annoncé ces faiblesses. Les fournisseurs de logiciels peuvent aussi diffuser des «rustines» appropriées que vous pouvez télécharger pour éliminer la faiblesse.

- Il importe de sensibiliser les membres de votre personnel aux signes indicateurs d'incidents de sécurité qui peuvent inclure les suivants :
  - demandes bizarres au téléphone portant spécialement sur de l'information;
  - visiteurs inhabituels;
  - tendances bizarres dans l'activité informatique;
  - apparence inhabituelle des écrans d'ordinateur;
  - ordinateurs qui prennent plus de temps que d'habitude pour exécuter des tâches de routine.
- Les membres de votre personnel doivent comprendre qu'il est toujours recommandé de prévenir la personne compétente s'ils observent quoi que ce soit qui pourrait être un signe indicateur d'incident de sécurité.
- Lorsqu'il se produit un incident de sécurité, les employés doivent savoir avec qui communiquer et comment le faire.
- Il faut mettre en œuvre un plan de reprise des activités en cas d'incident grave en matière de sécurité. Le plan doit préciser :
  - les personnes désignées qui interviennent dans la réponse;
  - des contacts à l'extérieur, y compris les services d'application de la loi, de lutte contre les incendies et, peut-être, des experts techniques;
  - des plans d'urgence à l'égard d'incidents prévisibles comme les suivants :
    - panne d'électricité;
    - catastrophes naturelles et accidents graves;
    - données compromises;
    - incapacité d'entrer sur les lieux;
    - perte d'employés essentiels;
    - panne de matériel.
    - Il faut diffuser votre plan à tous les employés et le tester au moins une fois par année, même si vous n'avez pas eu d'incident de sécurité.
- Après chaque incident à la suite duquel on utilise le plan, et après chaque essai, il faut revoir le plan et le mettre à jour au besoin en fonction des leçons apprises.
- La formation continue est vitale.

Contrôle de vérification et diligence raisonnable

Une bonne sécurité de l'information consiste notamment à savoir qui a accès à votre système et à pouvoir consigner ces événements d'accès. Vous devez aussi avoir un système qui permet d'assurer que l'on respecte vraiment vos procédures de sécurité. Il est essentiel de pouvoir vérifier et évaluer l'observation de la sécurité de l'information – on ne peut gérer ce qu'on ne peut mesurer!

- Il faut vérifier les aspects importants de votre sécurité, par exemple, qui a accès à vos systèmes et qui a utilisé quels renseignements.
- Vos dossiers doivent contenir chacune de vos procédures de sécurité. Par exemple, si votre procédure indique que vous vérifiez votre génératrice d'urgence une fois par semaine, quelqu'un doit signer un registre pour indiquer qu'on l'a fait. La tenue de bons dossiers est essentielle au contrôle de vérification.
- Des contrôles de vérification peuvent être nécessaires pour satisfaire des mesures législatives ou réglementaires. En tenant de bons dossiers, vous démontrez clairement que vous vous conformez à vos obligations.
- Une vérification doit assurer que les procédures que vous avez mises en place sont efficaces et pertinentes. C'est un éléments déclencheur qui pousse à réévaluer l'efficacité de vos normes et procédures sur la sécurité de l'information.
- Les vérifications sont efficaces seulement si l'on donne suite à leurs résultats et que l'on définit et met en œuvre les mesures qui s'imposent. Une bonne piste de vérification n'est pas simplement un exercice sur papier. Si quelque chose tourne mal, la piste doit vous révéler ce qui s'est passé et pourquoi, ce qui vous aidera à continuer d'améliorer la sécurité de votre entreprise.