CAN/DGSI 118:2023
NORME NATIONALE DU CANADA

Première édition
2023-11

Cybersécurité : cyberrésilience en santé

35.020; 35.030

- Page laissée intentionnellement vierge -

Table des matières

- Page laissée intentionnellement vierge -

Avant-propos

L'Institut des normes de gouvernance stratégique (INGN) élabore des normes de gouvernance de la technologie numérique adaptées à une utilisation planétaire. Il collabore avec des experts, avec des partenaires au pays et à l'étranger et avec le public pour établir des normes nationales visant à réduire les risques pour la population et les organisations canadiennes qui adoptent et utilisent des technologies novatrices dans l'économie numérique d'aujourd'hui.

Ses normes sont élaborées conformément aux *Exigences et lignes directrices – Accréditation des organismes d'élaboration de normes* (13 juin 2019) du Conseil canadien des normes (CCN).

Il est à noter que certains éléments de la présente norme peuvent faire l'objet de droits de brevet. L'INGN ne saurait être tenu responsable de ne pas avoir indiqué ces droits. Les droits de propriété intellectuelle répertoriés lors de l'élaboration du document figurent dans l'introduction.

Pour en savoir plus sur l'INGN :

Institut des normes de gouvernance numérique
500-1000, promenade Innovation
Ottawa (Ontario) K2K 3E7
www.dgc-cgn.org

Les Normes nationales du Canada sont élaborées par les organismes titulaires de l'accréditation du CCN, conformément aux exigences et lignes directrices de ce dernier. On trouvera des renseignements supplémentaires sur ces normes au www.ccn.ca.

Le CCN est une société d'État qui fait partie du portefeuille d'Innovation, Sciences et Développement économique Canada (ISDE). Pour améliorer la compétitivité économique du Canada et le bien-être collectif de sa population, le CCN dirige et facilite l'élaboration et l'utilisation de normes nationales et internationales. Il coordonne aussi la participation du pays à l'élaboration des normes et définit des stratégies pour promouvoir les efforts de normalisation canadiens.

Le CCN fournit des services d'accréditation à divers clients, dont des organismes de certification de produits, des laboratoires d'essai et des organismes d'élaboration de normes. La liste des programmes du CCN et des organismes accrédités peut être consultée sur le site www.ccn.ca.

- Page laissée intentionnellement vierge -

Introduction

Le présent document constitue la première version de la norme CAN/DGSI 118:2023, *Cybersécurité : cyberrésilience en santé*.

Cette norme a été élaborée par le comité technique 5 (TC 5) sur la cybersécurité de l'Institut des normes de gouvernance numérique, qui se compose de plus de 180 grands penseurs et experts en cybersécurité et en sujets connexes. Elle a été approuvée par un groupe avec droit de vote formé par le comité technique, comprenant quatre producteurs, trois utilisateurs, quatre représentants de la collectivité et quatre représentants du secteur public, d'organismes de réglementation ou d'organismes responsables des politiques.

Toutes les unités de mesure utilisées sont exprimées conformément au Système international d'unités (SI).

La norme sera soumise à l'examen du comité technique au plus tard un an après sa date de publication, après quoi elle pourra être rééditée, révisée, confirmée ou abandonnée.

Son but premier est énoncé sous la rubrique « Portée ». Il incombe néanmoins à l'utilisateur de juger si elle convient à une application donnée.

La norme est destinée à des fins d'évaluation de la conformité.

L'Institut des normes de gouvernance numérique remercie SoinsSanté*CAN* pour sa vision, son soutien et sa collaboration pour co-développer de la norme CAN/DGSI 118:2023, *Cybersécurité : cyberrésilience en santé*. SoinsSanté*CAN* est la voix pancanadienne d'appel à l'action des organisations de soins et des hôpitaux du Canada. L'organisme œuvre à promouvoir la recherche et l'innovation en santé, à améliorer la disponibilité des soins de grande qualité au pays et à fournir des programmes d'apprentissage inégalés aux professionnels de la santé. www.healthcarecan.ca/fr/

L'Institut des normes de gouvernance numérique reconnaît le soutien financier de Sécurité publique Canada.

Sécurité publique Canada | Public Safety Canada

ICS 03.100.01; 35.030

THIS NATIONAL STANDARD OF CANADA IS AVAILABLE IN BOTH FRENCH AND ENGLISH.

- Page laissée intentionnellement vierge -

Contexte

Les organisations de santé du Canada sont souvent les cibles de cyberattaques (escroquerie au faux ordre de virement, piratage psychologique, attaque par rançongiciel, vol de données, etc.). Les conséquences éventuelles sont multiples : panne des systèmes, problèmes opérationnels, retards et attente prolongée pour les patients, redirection des soins d'urgence ou critiques vers d'autres établissements, atteinte à la vie privée, perte de données, atteinte à l'intégrité des données et plus. Les organisations de santé n'ont pas les ressources pour mettre en place un cadre de cybersécurité rigoureux et des solutions technologiques novatrices, mais il leur est nécessaire de mettre en place des contrôles de base. C'est pourquoi la présente norme définit les mesures de cybersécurité les plus utiles.

L'annexe A offre plus de contexte ainsi que des exemples de brèches de sécurité informatique au sein d'organisations de santé.

Sécurité des soins de santé virtuels (visites virtuelles, suivis des patients à distance, applications pour les patients)

Visites virtuelles

Les visites virtuelles sont des rencontres cliniques entre un patient et un fournisseur de soins organisées à distance à l'aide d'outils électroniques divers, comme des plateformes de conférence téléphonique ou vidéo et des systèmes de messagerie ou de partage de documents sécurisés, pour faciliter la prestation des soins et en maximiser la qualité, l'efficience et l'efficacité. Une visite virtuelle peut être synchrone (communication en temps réel) ou asynchrone (communication intermittente entre le patient et le médecin). Chacun de ces outils amène ses propres risques de confidentialité et de sécurité qui ne sont pas présents dans les cliniques et les hôpitaux.

Suivi des patients à distance

Le suivi à distance consiste à utiliser des technologies pour surveiller et enregistrer les données de santé d'un patient à la maison ou dans un autre contexte non clinique pour améliorer sa qualité de vie et ses résultats de santé.

Les processus et les technologies (dispositifs et applications) utilisés peuvent appartenir à l'organisation de santé, ou à un tiers qui facilite la collecte de renseignements médicaux dans les milieux non cliniques contrôlés par les patients et leur consolidation dans un point central conçu ou géré par l'organisation.

Dans certains cas, les outils de suivi peuvent être considérés comme des dispositifs médicaux. Les organismes de réglementation du Canada et des États-Unis ont publié des lignes directrices pour baliser les définitions des dispositifs médicaux, leur usage prévu et les risques de préjudice associés à leur emploi. Santé Canada tient notamment un site Web consacré à ces documents d'orientation, et le Secrétariat américain aux produits alimentaires et pharmaceutiques (FDA) a publié à ce sujet le guide Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff le 25 septembre 2013.

Les dispositifs et applications de suivi des patients à distance mentionnés plus haut présentent des risques uniques, dont les organisations de santé devraient tenir compte au moment de choisir les applications mobiles à utiliser.

Sécurité des technologies de santé (infonuagique, Internet des objets, systèmes vieillissants) et des technologies opérationnelles

Comme les risques de cybersécurité associés aux dispositifs médicaux évoluent constamment, il n'est pas possible de tous les éliminer à l'étape d'installation. Les organisations peuvent gérer ces risques en instaurant un programme de gestion des risques indépendant ou parallèle visant à prévenir, à surveiller et à pallier les vulnérabilités des dispositifs médicaux, soit les dispositifs reliés à l'Internet des objets (IdO) (ex. : appareil de radiographie) et les objets personnels connectés utilisant un protocole Ethernet, Bluetooth, Wi-Fi ou autre.

De plus en plus, les organisations de santé se tournent vers les technologies opérationnelles (TO) interconnectées aux TI et à l'IdO pour soutenir l'environnement physique. Aussi auront-elles besoin d'un cadre de sécurité approprié pour protéger les données recueillies par ces TO et pour assurer la disponibilité et la fiabilité de la technologie. Les stratégies de cyberrésilience présentées dans la présente norme s'appliquent tant aux TI qu'aux TO. Il sera également important de sécuriser les solutions d'intelligence artificielle (IA) et d'apprentissage machine dans les environnements de TO.

Cybersécurité : cyberrésilience en santé

1 Portée

La présente norme définit les exigences minimales de cybersécurité pour les organisations de santé et favorise la cyberrésilience du système de santé canadien.

NOTE : On recommande aux organisations de considérer la sécurité physique comme un élément essentiel de leur programme de cybersécurité, mais compte tenu de la complexité de la tâche et des ressources nécessaires, ce travail dépasse la portée de la présente norme.

2 Références normatives

La présente norme renvoie au document ci-dessous de telle sorte qu'une partie ou la totalité de son contenu constitue une exigence normative. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, c'est la dernière édition (y compris les éventuelles modifications) qui s'applique.

CAN/CIOSC 104:2021, *Contrôles de cybersécurité de base des petites et moyennes organisations*

3 Termes et définitions

Voici les termes et définitions qui s'appliquent pour les besoins du présent document :

accès non autorisé
Accès physique ou logique à un réseau, à un système ou à des données sans autorisation.

accès protégé Wi-Fi
Protocole de sécurité et programme de certification de la sécurité conçus par la Wi-Fi Alliance pour protéger les réseaux informatiques sans fil.

[SOURCE : ISO 20415:2019]

application
Logiciel ou programme qui apporte une solution à un problème d'application.

[SOURCE : ISO/IEC 20944-1:2013]

application de correctifs
Mise à jour d'un logiciel ou d'un micrologiciel.

atteinte à la protection des données
Perte de renseignements personnels ou consultation ou divulgation non autorisée de tels renseignements en raison d'une faille dans la sécurité, plus particulièrement dans la cybersécurité pour les besoins du présent document.

atteinte à la vie privée
Collecte, utilisation ou divulgation non autorisées de renseignements personnels médicaux et autres (ex. : vol ou perte de données, copie, modification ou élimination non autorisées).

authentification multifacteur
Méthode d'*authentification* qui exige, pour vérifier l'identité de l'utilisateur, une combinaison d'au moins deux facteurs. Il peut s'agir de choses que l'utilisateur connaît (ex. : mot de passe) ou possède (ex. : jeton physique), ou d'attributs physiques (ex. : biométrie).

chiffrement
Procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées.

[SOURCE : Centre canadien pour la cybersécurité]

code gris
Code utilisé en cas de perte d'un système essentiel (électricité, eau, chauffage, gaz médicaux, communications, rançongiciel, technologies de l'information, etc.) ou de situation pouvant poser un risque de santé et sécurité pour les personnes présentes dans l'hôpital (ex. : personne agressive).

code malveillant
Programme ou code écrit pour recueillir de l'information sur un système ou un utilisateur, détruire les données d'un système, faciliter une intrusion plus en profondeur, falsifier des données ou des rapports de système, ou créer des nuisances ralentissant les opérations d'un système et les activités du personnel de maintenance.

NOTE 1 : Une attaque par code malveillant peut prendre la forme d'un virus, d'un ver informatique, d'un cheval de Troie ou d'autres exploits automatisés.

NOTE 2 : Les codes malveillants sont aussi souvent appelés « maliciels ».

[SOURCE : IEC/TS 62443-1-1:2009]

confidentialité
Capacité à protéger l'information sensible contre les accès non autorisés.

contrôle correctif de cybersécurité
Mesure de protection ou de prévention déployée en l'absence ou en remplacement de contrôles intégrés du fabricant d'un dispositif médical. Il s'agit de contrôles externes configurables sur le terrain à l'intention d'un utilisateur qui offrent au dispositif une cyberprotection supplémentaire ou comparable.

cyberrésilience
Capacité d'une entité à se préparer aux cyberattaques, à les prévenir et à continuer d'obtenir les résultats escomptés malgré les incidents. Il s'agit d'une caractéristique cruciale pour les systèmes de TI, les infrastructures essentielles, les processus opérationnels, les organisations, les sociétés et les États-nations.

défaillance du réseau (généralisée)
Incident portant atteinte à la confidentialité, à l'intégrité ou à la disponibilité d'un réseau.

défaillance du système d'applications
Incident portant atteinte à la confidentialité, à l'intégrité ou à la disponibilité des applications.

déni de service
Voir « interruption de service ».

devrait/devraient
Indication d'une possibilité de choix avec une préférence marquée; équivalent à « il est fortement recommandé ».

divulgation non autorisée
Incident portant atteinte à la confidentialité, à l'intégrité ou à la disponibilité de données.

doit/doivent
Indication d'une exigence pour la conception ou l'application d'une méthode d'essai.

données
Renseignements recueillis dans le cadre des pratiques normales, notamment l'information structurée ou non structurée générée par les systèmes de production et de non-production.

droit d'accès minimal
Principe selon lequel il convient de n'accorder aux utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches qui leur ont été dûment attribuées. Ce principe permet de limiter les dommages pouvant résulter d'une utilisation non autorisée – abusive ou accidentelle – d'un système d'information.

[SOURCE : Centre canadien pour la cybersécurité]

gestionnaire de mots de passe
Programme informatique permettant aux utilisateurs de stocker, de créer et de gérer des mots de passe pour des applications locales et des services en ligne. Un gestionnaire de mots de passe facilite la génération et l'utilisation de mots de passe complexes, soit en les conservant dans une base de données chiffrée, soit en les calculant sur demande.

hameçonnage
Attaque reposant sur un appel téléphonique, un message texte, un courriel ou un média social pour convaincre quelqu'un de cliquer sur un lien malveillant, de télécharger un maliciel ou de révéler une information sensible. Les tentatives d'hameçonnage prennent souvent la forme de messages de masse prétendant provenir d'une source fiable (ex. : banque, service de courrier).

[SOURCE : Centre canadien pour la cybersécurité]

harponnage
Attaque d'hameçonnage visant une personne, un groupe ou une organisation en particulier et

utilisant des renseignements personnels ou professionnels pour pousser la victime à répondre, à cliquer sur un lien ou à ouvrir une pièce jointe.

[SOURCE : Centre canadien pour la cybersécurité]

incident de cybersécurité
Tentative non autorisée, réussie ou non, d'accéder à une ressource de système ou à un réseau informatique, de le modifier, de le détruire, de le supprimer ou de le rendre inutilisable.

[SOURCE : CAN/CIOSC 104:2021]

information sensible
Information devant être protégée contre les pertes, les modifications et les divulgations non autorisées.

NOTE : Il peut s'agir de renseignements personnels, d'information commerciale ou d'information classifiée.

intégrité
Capacité à protéger l'information contre la modification et la suppression non autorisées.

interruption de service
Incident empêchant l'accès à un service ou perturbant autrement son fonctionnement normal.

maliciel
Logiciel malveillant conçu pour infiltrer ou endommager un système informatique. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.

[SOURCE : Glossaire du Centre canadien pour la cybersécurité]

organisation de santé
Organisation contribuant directement ou indirectement à la prestation de soins de santé.

NOTE : Tout simplement « organisation » pour les besoins de la présente norme.

[SOURCE : ISO 22886:2020]

OWASP
Open Web Application Security Project (projet ouvert de sécurité des applications Web).

pare-feu
Barrière de sécurité entre deux périmètres contrôlant le volume et les types de trafic autorisés à passer de l'un à l'autre.

perte d'information
Voir « divulgation non autorisée ».

peut/peuvent
Indication d'une possibilité de choix avec une préférence sous-entendue.

plan d'intervention en cas d'incident
Document définissant les processus, les procédures et les documents liés à la réaction d'un organisme à un incident, c'est-à-dire les mesures de détection et de gestion de l'incident et de reprise des activités. Les cybermenaces, les catastrophes naturelles et les pannes imprévues sont des exemples d'incidents qui se répercuteront sur les réseaux, les systèmes et les dispositifs.

[SOURCE : Centre canadien pour la cybersécurité]

préjudice
Dommage subi par une organisation lorsque ses systèmes et actifs informatiques sont compromis.

rançongiciel
Type de *maliciel* empêchant un utilisateur d'accéder à un système ou à des données jusqu'à ce qu'il ait payé une rançon, en biens virtuels ou réels ou en argent.

réseau local sans fil (WLAN)/Wi-Fi
Technologie de réseautage local sans fil qui permet la connexion d'appareils électroniques au réseau, principalement au moyen des bandes radio de 2,5 GHz et de 5 GHz.

NOTE 1 : « Wi-Fi » est une marque de commerce de la Wi-Fi Alliance.

NOTE 2 : « Wi-Fi » est couramment utilisé comme synonyme de « WLAN », puisque la plupart des réseaux WLAN modernes reposent sur les normes du Wi-Fi.

[SOURCE : ISO/IEC 27033-6:2016]

sécurité des supports amovibles
Sécurité d'un support amovible (ex. : clé USB, ordinateur portable, tablette).

soins virtuels
Utilisation de technologies de l'information et des communications pour fournir des soins de santé et des recommandations aux patients sans que ces derniers et le médecin aient à se rencontrer physiquement. Ces technologies ne constituent pas en elles-mêmes des traitements ni des interventions de santé virtuelles; ce sont simplement des outils qui améliorent l'accessibilité et l'efficacité des soins et facilitent les soins axés sur la personne et les échanges d'information.

[SOURCE : CAN/HSO 83001:2018]

système de noms de domaine (DNS)
Nomenclature distribuée et hiérarchisée mondiale servant à identifier les entités connectées à Internet.

NOTE : Les domaines de premier niveau sont au sommet de la hiérarchie.

[SOURCE : ISO/TR 14873:2013]

technologies opérationnelles (TO)
Systèmes programmables ou appareils gérés qui interagissent avec l'environnement physique. Ces technologies détectent ou causent des changements directs en surveillant et en contrôlant les appareils, les processus et les événements. Il peut s'agir d'appareils de radiographie, de dialyse, de surveillance des patients, de simulation, etc.

[SOURCE : NIST 800-37 Rev 2 (modifiée)]

TI
Technologies de l'information.

utilisation non autorisée
Utilisation physique ou logique d'un réseau, d'un système ou de données sans autorisation.

visite virtuelle
Rencontre clinique entre un patient et un fournisseur de soins organisée à distance à l'aide d'outils électroniques divers, comme des plateformes de conférence téléphonique ou vidéo et des systèmes de messagerie ou de partage de documents sécurisés, pour faciliter la prestation des soins et en maximiser la qualité, l'efficience et l'efficacité. Une visite virtuelle peut être synchrone (communication en temps réel) ou asynchrone (communication intermittente entre le patient et le médecin).

4 Gestion des risques organisationnels

4.1 Direction

4.1.1 La direction de l'organisation est ultimement responsable du programme de cybersécurité.

4.1.2 Pour démontrer l'importance qu'elle accorde à la cybersécurité, elle doit établir des politiques et des objectifs en la matière cohérents avec son orientation stratégique.

4.1.3 Elle doit aussi veiller à la disponibilité des ressources (ex. : personnes, processus, technologies, fonds, pouvoirs) nécessaires au programme de cybersécurité et à leur harmonisation avec les politiques et les objectifs de cybersécurité.

4.1.4 La direction doit communiquer l'importance d'une cybersécurité efficace et du respect des exigences du programme de cybersécurité.

4.1.5 Elle doit fixer le degré de cyberrisque ciblé pour l'organisation.

4.1.6 Elle doit établir des indicateurs pour le programme de cybersécurité et faire un suivi continu des progrès.

4.1.7 Enfin, elle doit aider les autres gestionnaires concernés à faire preuve de leadership dans leurs propres domaines de responsabilité.

4.2 Délégation de la sécurité

4.2.1 La direction doit nommer un membre de l'équipe de haute gestion pour surveiller la cybersécurité de l'organisation et en rendre compte. Voici ses responsabilités en ce sens :

a. Élaborer et mettre en place un programme de cybersécurité à l'échelle de l'organisation qui couvre les contrôles de base.

b. Rédiger et diffuser des politiques et procédures de sécurité de l'information.

c. Coordonner la création et la mise en place d'un programme organisationnel de sensibilisation et de formation sur la sécurité de l'information.

d. Déterminer le degré de cyberrisque ciblé pour l'organisation et transmettre une recommandation à cet effet à la direction.

e. Suivre les progrès vers la cible et rendre régulièrement des comptes sur l'avancement.

f. Coordonner l'intervention en cas d'atteinte réelle ou présumée à la confidentialité, à l'intégrité ou à la disponibilité des systèmes et des données de l'organisation.

g. Recenser les risques organisationnels et en prioriser l'atténuation selon leur probabilité et la gravité de leurs répercussions potentielles.

h. Participer à des groupes d'échange d'information ou instaurer un programme de formation ou une autre façon de demeurer à l'affût des cybermenaces émergentes.

i. Déléguer les fonctions de sécurité de l'information au besoin.

NOTE : Voir la matrice RACI (annexe E).

4.3 Évaluation des risques pour les actifs

4.3.1 L'organisation doit dresser l'inventaire de ses actifs de TI (infrastructure, applications et données) et de TO (ex. : appareils de radiographie, de dialyse, de surveillance des patients) et les classer selon leur degré d'importance pour ses activités.

4.3.2 Elle doit déterminer les actifs à protéger en priorité.

4.3.3 L'organisation doit réaliser une évaluation des risques de cybersécurité pour cerner les menaces et les vulnérabilités préoccupantes et établir des contrôles de sécurité appropriés pour veiller à la continuité des services des actifs essentiels.

4.3.4 L'organisation devrait harmoniser ses pratiques avec les normes de gestion des risques existantes.

4.3.5 L'organisation doit tenir à jour des diagrammes et des descriptions de flux de données couvrant les mesures de sécurité et de protection de la vie privée sur l'ensemble du cycle de vie des renseignements médicaux personnels : création ou collecte, transfert, utilisation, stockage et destruction.

NOTE 1 : Certains gouvernements imposent des exigences de souveraineté des données, par exemple que tous les renseignements médicaux personnels demeurent dans la province ou au Canada. Il est donc important de savoir dans quel pays les données sont stockées. La période de rétention des données en mouvement devrait être connue et réduite au minimum.

NOTE 2 : À mesure que les applications de santé migrent vers l'infonuagique, l'emplacement géographique des données devra être ajouté aux diagrammes et aux descriptions de flux de données.

4.4 Gestion des identités et de l'accès

4.4.1 Tous les systèmes d'information donnant accès à des renseignements médicaux personnels doivent vérifier l'identité systématiquement.

4.4.2 L'organisation doit faire passer les utilisateurs potentiels de ses systèmes de santé par un processus d'inscription comprenant une vérification d'une pièce d'identité gouvernementale avec photo et de l'adhésion à l'ordre approprié (le cas échéant).

NOTE : Les exigences minimales peuvent comprendre une vérification des méthodes de communication avec l'utilisateur (téléphone, courriel), l'intégration de programmes gouvernementaux d'identité numérique ou d'autres mesures de validation lorsqu'il est impossible de vérifier physiquement une carte d'identité gouvernementale avec photo.

4.4.3 L'organisation doit mettre en place un processus défini pour vérifier régulièrement tous les droits d'accès et les révoquer ou modifier rapidement au besoin.

4.4.4 Elle doit munir les comptes des utilisateurs de contrôles ne permettant que les accès nécessaires au travail de ceux-ci et restreindre les privilèges d'administrateur à ceux qui en ont besoin.

4.4.5 Elle doit aussi examiner la possibilité de mettre en place un système centralisé de contrôle d'accès.

4.4.6 Elle doit instaurer l'authentification multifacteur, ou consigner toute situation où elle est incapable de le faire ou décide de ne pas le faire.

4.4.7 Elle doit suivre un processus de vérification et d'approbation officiel ne permettant qu'aux utilisateurs autorisés d'accéder aux TO essentielles.

4.5 Outils de visibilité

4.5.1 L'organisation devrait instaurer dans les environnements de TI et de TO un système de détection et d'intervention aux terminaux et y intégrer des processus de gestion de l'information et des événements de sécurité ainsi qu'une équipe d'intervention en cas d'incident.

4.5.2 Elle devrait aussi mettre en place des systèmes d'information et de gestion relativement aux menaces.

4.5.3 Elle doit adopter des mécanismes de vérification efficaces pour reconstruire toutes les manipulations (création, lecture, modification, suppression et partage) effectuées sur ses données sensibles.

5 Formation (cyberrésilience de l'effectif)

5.1 Sensibilisation et formation sur la cybersécurité

5.1.1 L'organisation doit former ses employés sur les pratiques de sécurité de base en se concentrant sur quelques mesures concrètes et faciles à appliquer pour protéger adéquatement les données, les systèmes et les appareils :

a. Utilisation de politiques de mot de passe efficaces

b. Repérage des courriels et des liens malveillants

c. Utilisation de logiciels approuvés

d. Utilisation appropriée d'Internet

e. Protection des TO contre les cybermenaces

f. Utilisation sécuritaire des médias sociaux

g. Traitement sécuritaire des données en fonction de leur sensibilité

NOTE 1 : Un programme de sensibilisation et de formation sur la cybersécurité efficace doit être appuyé de politiques.

NOTE 2 : Cette liste n'est pas exhaustive; il ne s'agit que d'exemples.

NOTE 3 : La sensibilisation et la formation sur la cybersécurité devraient être adaptées selon les rôles et les responsabilités des différents utilisateurs et employés.

NOTE 4 : L'ensemble du personnel doit être avisé des lois locales pertinentes.

5.1.2 L'organisation doit élaborer, mettre par écrit et diffuser un programme de formation à la confidentialité et à la sécurité pour les utilisateurs des systèmes d'information.

a. Les utilisateurs doivent suivre la formation avant d'avoir accès aux systèmes pour la première fois, puis une fois par an.

b. La formation doit être mise à jour en fonction des nouvelles menaces.

c. Les acquis doivent être confirmés à l'aide d'un test avec une note de passage minimale.

NOTE 1 : La formation devrait couvrir les pratiques exemplaires en matière d'identifiants (voir plus bas); le repérage des courriels et des liens malveillants, l'utilisation de logiciels approuvés, l'utilisation appropriée d'Internet, la protection des données, des systèmes d'information et des appareils, et l'utilisation sécuritaire des médias sociaux.

NOTE 2 : Il n'est pas toujours faisable d'imposer une formation sur la confidentialité et la sécurité à tous les employés, mais la politique doit englober toutes les personnes (employés, sous-traitants, directeurs, chercheurs, étudiants, bénévoles, etc.) qui ont accès à des renseignements médicaux personnels ou à des données opérationnelles confidentielles, ou qui sont raisonnablement susceptibles d'avoir une incidence sur la sécurité de systèmes contenant de tels renseignements. Des conséquences doivent s'appliquer si la formation n'est pas suivie.

NOTE 3 : Dans certains cas, les médecins sont légalement indépendants de la clinique ou de l'hôpital où ils exercent, ce qui peut compliquer l'application d'une exigence de test. Pour contourner le problème, les organisations peuvent prendre des dispositions contractuelles exigeant des médecins qu'ils suivent la formation à la fréquence définie et respectent la politique de sécurité, y compris qu'ils utilisent une adresse courriel reliée à un système de validation des fournisseurs approprié conforme aux cadres de confidentialité pertinents.

NOTE 4 : Les lois sur la protection des renseignements personnels des différentes provinces peuvent poser des exigences supplémentaires, qui doivent être intégrées à la formation sur la confidentialité et la sécurité. Les organisations devraient communiquer avec leur responsable de la confidentialité pour en savoir plus sur les exigences de toutes les provinces où elles sont établies ou offrent des services.

5.1.3 Le programme de sensibilisation à la sécurité doit couvrir les pratiques exemplaires pour prévenir le partage d'identifiants, de mots de passe ou d'autres accès aux systèmes de renseignements médicaux, et ce, peu importe les processus d'authentification en place.

NOTE : Les milieux de travail en santé ne se prêtent pas toujours à l'utilisation de mots de passe. Par exemple, un médecin peut difficilement utiliser un clavier en salle d'opération. Alors, d'autres méthodes d'authentification, comme des cartes à puce, peuvent être utilisées. L'objectif de la présente exigence est de s'assurer que les utilisateurs recevront la consigne de ne pas partager leurs authentifiants, quels qu'ils soient. Autre exemple : les médecins en milieu clinique ne doivent jamais permettre au personnel administratif ou aux médecins suppléants d'utiliser leurs identifiants pour accéder aux systèmes d'information. Chaque utilisateur autorisé doit avoir son propre compte, configuré en fonction des accès dont il a besoin pour son travail.

5.2 Hameçonnage

5.2.1 Toute organisation qui utilise des services de courriel doit mettre en place un programme de formation continue sur les techniques de piratage psychologique, comme l'hameçonnage, l'hameçonnage vocal, le harponnage et l'escroquerie au faux ordre de virement.

NOTE : Il n'est pas toujours possible de procéder à une simulation d'hameçonnage, par exemple parce que les médecins utilisent des adresses courriel personnelles. Dans ces cas, l'organisation peut avoir recours à des méthodes de sensibilisation traditionnelles et ajouter l'hameçonnage aux sujets de la formation.

5.3 Hygiène des identifiants

5.3.1 L'organisation doit incorporer des pratiques d'hygiène des identifiants à son programme de formation sur la sécurité.

5.3.2 Elle doit aussi avoir recours à un gestionnaire de mots de passe.

5.3.3 Elle doit utiliser les meilleurs outils adaptés à ses systèmes pour vérifier la robustesse des mots de passe et y jumeler des mécanismes d'authentification multifacteur autant que possible.

5.3.4 L'organisation doit exiger la modification du mot de passe dans tous les cas présumés ou prouvés de compromission.

6 Contrôles technologiques

6.1 Protection des données

6.1.1 L'organisation doit mettre en place des contrôles pour détecter et prévenir les fuites et la perte de données.

6.1.2 Elle doit veiller à ce que le transfert de données sensibles (ex. : renseignements médicaux personnels) d'une infrastructure locale à un environnement infonuagique se fasse en toute sécurité, pendant les transferts initiaux et pendant les mises à jour des dossiers hybrides.

NOTE : À mesure que les services passent à l'infonuagique, il est important de protéger les données que contiennent ces environnements. De nombreux fournisseurs permettent d'ailleurs de chiffrer les données à l'aide de clés gérées par le client pour éviter l'exposition de données sensibles aux administrateurs du nuage.

6.1.3 L'organisation doit se doter d'une procédure pour évaluer les différentes méthodes de chiffrement des données sensibles transférées, entreposées et utilisées.

6.1.4 Elle doit appliquer des pratiques de cryptage conformes aux normes sectorielles pour s'assurer que les données recueillies et stockées par les TO et les dispositifs médicaux sont protégées en tout temps, sur les dispositifs et lors du transfert vers d'autres environnements de TI (ex. : nuage).

6.2 Réduction de l'utilisation des renseignements médicaux personnels

6.2.1 L'organisation doit avoir des environnements de test distincts des environnements de production.

6.2.2 Elle doit tâcher de réduire, voire d'éliminer l'utilisation de données de production dans les environnements de préproduction.

6.2.3 S'il est impossible d'éliminer les données de production d'un environnement de préproduction, celui-ci doit être doté de contrôles de sécurité égaux ou supérieurs à ceux de l'environnement de production.

NOTE : Certains gouvernements imposent des exigences pour les méthodes de dépersonnalisation des renseignements personnels (médicaux et autres) et le consentement à l'utilisation de renseignements dépersonnalisés. Renseignez-vous auprès de votre conseiller juridique ou de votre responsable de la confidentialité.

6.2.4 Les données de production sensibles employées dans l'environnement de test doivent être anonymisées autant que possible.

6.3 Copies de sauvegarde

6.3.1 L'organisation doit faire des copies de tous ses renseignements, y compris ses renseignements personnels – médicaux et autres –, et s'assurer que ces copies sont sauvegardées, tenues à jour et contrôlées comme il se doit.

6.3.2 Les copies contenant des renseignements médicaux personnels doivent être stockées sous forme chiffrée.

6.3.3 L'organisation doit sauvegarder ses systèmes contenant des données opérationnelles essentielles et voir au fonctionnement adéquat et efficace de ses mécanismes de reprise.

6.3.4 Elle doit remplacer régulièrement les sauvegardes et les conserver dans un emplacement externe sécurisé (lieu physique ou service infonuagique) pour être en mesure de les récupérer en cas de catastrophe (incendie, inondation, tremblement de terre ou incident de cybersécurité localisé).

6.3.5 Elle doit aussi s'assurer que ses plans de résilience définissent les exigences d'impartition du processus de recrutement et les objectifs de temps de reprise pour tous les systèmes essentiels.

6.3.6 L'objectif de point de rétablissement doit tenir compte des répercussions sur la sécurité des patients si les données ne sont pas parfaitement à jour.

6.3.7 Les objectifs de temps de reprise devraient également tenir compte des répercussions sur la sécurité des patients et la continuité des soins si les données des patients devenaient inaccessibles.

6.3.8 Les plans de résilience doivent définir des solutions de rechange au cas où les objectifs de temps de reprise ne pourraient être respectés.

6.3.9 L'organisation doit configurer ses systèmes de TO essentiels de façon à ce que les paramètres et les données soient sauvegardés de manière sécuritaire.

6.3.10 Elle doit réaliser des tests réguliers sur toutes ses sauvegardes de données pour valider les procédures de sauvegarde et de reprise.

6.4 Résilience (disponibilité)

6.4.1 Le programme de résilience de l'organisation doit comprendre, au minimum, des plans de continuité des activités, de communication en situation de crise, de reprise après sinistre et d'intervention en cas de cyberincident.

6.4.2 L'organisation doit définir le temps d'indisponibilité maximum tolérable, les objectifs de temps de reprise (OTR) et les objectifs de point de rétablissement (OPR) en fonction du caractère essentiel des systèmes, des conséquences d'une éventuelle panne et de ses ressources disponibles.

6.4.3 Elle doit avoir des sauvegardes, des configurations et des stratégies de reprise adéquates (centres de relève immédiate, centres de relève, salles blanches, écriture miroir, sauvegardes infonuagiques vs physiques) correspondant aux OTR et aux OPR de chaque système pour prévenir les pannes et les périodes d'indisponibilité injustifiées.

6.4.4 Elle doit assurer la continuité de son programme de résilience en réalisant des exercices et des tests réguliers pour confirmer les OTR et les OPR et actualiser ses plans en conséquence.

6.5 Documentation et plans de reprise pour tous les systèmes essentiels

6.5.1 L'organisation doit prévoir le rétablissement des systèmes à un état défini dans l'impartition du processus de recrutement et les objectifs de temps de reprise après une interruption, une compromission ou une panne.

6.5.2 Elle doit s'assurer que les plans de reprise sont exécutés pendant ou après un incident de cybersécurité.

6.5.3 Elle doit s'assurer que la conception, la documentation et les plans de reprise de ses systèmes essentiels tiennent compte des objectifs de temps de reprise et des objectifs de point de rétablissement.

6.6 Exercices de reprise après sinistre

6.6.1 L'organisation doit procéder régulièrement à des exercices et à des tests de reprise.

6.6.2 Elle doit aussi tester régulièrement ses procédures de reprise sur un échantillon des données sauvegardées pour vérifier l'intégrité de l'ensemble du processus de sauvegarde et de restauration.

6.6.3 Elle doit déterminer au cas par cas quels sont les logiciels et les données (y compris l'information sensible) essentiels à son fonctionnement et leur fréquence de modification.

NOTE : Par exemple, les postes de travail et les serveurs essentiels peuvent nécessiter des sauvegardes incrémentielles quotidiennes, alors que les postes de travail de base peuvent être récupérés à partir d'une même image.

6.6.4 Comme les exigences de sauvegarde et de reprise sont uniques à chaque système, l'organisation doit établir au cas par cas la nécessité d'une copie et, le cas échéant, la fréquence de sauvegarde.

6.6.5 Elle doit sauvegarder ses systèmes contenant des données opérationnelles essentielles et voir au fonctionnement adéquat et efficace de ses mécanismes de reprise.

6.6.6 Elle devrait envisager de chiffrer ses sauvegardes avec une clé récupérable conservée en sécurité. La clé et les sauvegardes non chiffrées devraient être conservées en sécurité et n'être accessibles qu'aux employés ou agents autorisés.

6.6.7 L'organisation doit tester régulièrement ses procédures de reprise sur un échantillon des données sauvegardées pour vérifier l'intégrité de l'ensemble du processus de sauvegarde et de restauration.

6.6.8 Enfin, elle doit s'assurer que les exercices de reprise se font sans exposer les données de production.

7 Considérations relatives aux technologies en santé

7.1 Considérations relatives aux logiciels

7.1.1 L'organisation doit installer les correctifs de confidentialité et de sécurité des données pour l'ensemble de ses logiciels et de son matériel afin de protéger ses actifs contre les vulnérabilités connues.

NOTE : Ceci comprend la gestion des correctifs s'appliquant aux systèmes de TI essentiels et aux systèmes de TO.

7.1.2 L'organisation doit activer la mise à jour automatique de l'ensemble de ses logiciels et de son matériel, lorsqu'il est possible de le faire en toute sécurité, et consigner tous les cas où elle décide de ne pas le faire.

NOTE : Ceci comprend la totalité des serveurs, des ordinateurs portables et de bureau, des tablettes, des téléphones cellulaires, de l'équipement réseau et des dispositifs médicaux.

7.1.3 L'organisation doit disposer d'une procédure assurant la mise à jour manuelle régulière des logiciels et du matériel ne pouvant être mis à jour automatiquement.

7.1.4 L'organisation peut établir une procédure d'essai pour assurer que les correctifs ne causent aucune perturbation et ne posent aucun danger pour les patients dans les cas où l'analyse des risques détermine qu'il s'agit d'une mesure judicieuse de réduction des risques.

7.2 Contrôles des réseaux

7.2.1 L'organisation doit instaurer des stratégies de protection des réseaux appropriées : pare-feu; sécurité des ports; contrôle des accès aux réseaux, à distance et sans fil; modèle à vérification systématique; sécurité du réseau infonuagique; etc.

7.2.2 Elle doit séparer ses différents réseaux, dont ceux utilisés pour les technologies de soins, pour les TO et pour les TI, afin de prévenir les accès latéraux malveillants ou non autorisés.

7.3 Technologies désuètes et contrôle correctifs

7.3.1 L'organisation doit obtenir et consulter les rapports périodiques *des autorités compétentes ou des fournisseurs autorisés avant la mise en marché* sur les vulnérabilités liées à la cybersécurité, le remplacement des appareils et les contrôles correctifs à mettre en place.

NOTE : Les autorités compétentes comprennent *Santé Canada (pour les dispositifs médicaux approuvés au Canada) et le FDA (aux États-Unis).*

7.3.2 L'organisation doit effectuer une évaluation des risques pour déterminer s'il y a lieu de remplacer les systèmes pour lesquels la mise à jour est impossible.

7.3.3 Un plan de traitement du risque est requis pour consigner les contrôles correctifs visant à réduire les risques liés au maintien des technologies désuètes.

7.4 Infonuagique

7.4.1 L'organisation doit déterminer les risques associés à son utilisation de fournisseurs ou de services infonuagiques et de services de TI externalisés et évaluer son seuil de tolérance au risque quant aux méthodes utilisées par ses fournisseurs pour accéder à l'information sensible et traiter celle-ci.

NOTE : Une organisation a généralement recours à un fournisseur tiers de services de TI ou de services gérés pour ses besoins de stockage et de traitement infonuagiques, la gestion ou l'hébergement de son site Web et la gestion de ses systèmes de paiement en ligne. Il est important qu'elle tienne compte de son seuil de tolérance aux risques quant à la réglementation en vigueur aux endroits où ses fournisseurs stockent ou utilisent son information sensible.

7.4.2 L'organisation qui utilise des services infonuagiques ou des services de TI externalisés doit :

a. exiger de ses fournisseurs de services infonuagiques qu'ils présentent un rapport SSAE 18 de l'Association of International Certified Professional Accountants (AICPA) ou un document équivalent indiquant qu'ils se conforment aux principes des services Trust, ou une analyse documentée expliquant pourquoi ils ne le font pas;

   NOTE : C'est l'organisation qui détermine l'équivalence avec la norme SSAE 18 de l'AICPA.

b. évaluer son seuil de tolérance aux risques quant aux régimes juridiques applicables au stockage et à l'utilisation de son information sensible par ses fournisseurs;

c. veiller à ce que son infrastructure de TI et ses utilisateurs communiquent de façon sécurisée avec les applications et services infonuagiques;

d. veiller à ce que les comptes administrateur des services infonuagiques utilisent une méthode d'authentification multifacteur et soient différents des comptes administrateur internes;

e. veiller au respect des lois locales et sur la résidence des données;

f. assurer l'utilisation de méthodes adéquates pour la suppression des données;

g. vérifier que les modalités des services infonuagiques ne permettent pas aux fournisseurs d'utiliser les données à d'autres fins;

h. veiller à ce que les accès des administrateurs du nuage soient restreints (sur permission de l'organisation seulement) et audités.

7.4.3 L'organisation qui utilise des services infonuagiques ou des services de TI externalisés doit réaliser une évaluation des facteurs relatifs à la vie privée et instaurer un processus de gestion des vulnérabilités.

7.4.3 Elle doit établir une procédure pour examiner régulièrement ses systèmes infonuagiques, y compris les contrôles de sécurité et de confidentialité et les lignes directrices de renforcement. Les exceptions doivent être mises par écrit.

7.5 Approvisionnement, gestion des fournisseurs et chaîne d'approvisionnement

7.5.1 Le processus d'approvisionnement de l'organisation doit comprendre une évaluation des risques de sécurité exhaustive portant notamment sur ce qui suit :

a. Gestion de l'accès aux données stockées dans des solutions infonuagiques ou de tiers;

b. Méthodes de chiffrement et gestion des clés de chiffrement;

c. Responsabilités et procédures liées à l'intervention en cas d'incident, à la gestion des incidents et aux avis, qui doivent être conformes aux principes de diligence requise;

d. Procédures de sauvegarde et de reprise après sinistre, y compris le site de basculement et son emplacement;

e. Sous-traitants qui peuvent avoir accès aux données ou à l'environnement, et principes de diligence requise les concernant;

f. Métadonnées pouvant être suivies et utilisées sans autorisation;

g. Démonstration de la conformité des tiers à des normes de sécurité et de leur obtention de certifications de sécurité;

h. Engagement à l'égard de l'innovation et du développement continus pour rester à l'affût des exigences de sécurité des normes sectorielles.

7.5.2 Dans son entente-cadre de service, l'organisation doit s'assurer que ses pratiques de sécurité sont vérifiables, et que les pratiques des tiers créent un profil de risque conforme aux lois et règlements sur la protection des renseignements médicaux.

7.5.3 Les nouvelles ententes avec les fournisseurs doivent comprendre des exigences relatives aux risques à la sécurité de l'information découlant des services ou de la manipulation, du traitement et de la communication de l'information, y compris les risques pour l'information et l'environnement de l'organisation, et toute exigence légale ou réglementaire.

7.5.4 Les nouvelles ententes avec les fournisseurs externes qui traitent ou stockent de l'information, fournissent des systèmes d'information ou des composants, ou ont accès à ces éléments doivent respecter les exigences de sécurité de l'organisation et faire l'objet d'un accord juridique.

7.5.5 Les types d'accès donnés aux tiers (ex. : fournisseurs de services de TI, développeurs de logiciels, services financiers) devraient être définis et consignés.

7.5.6 L'accès au réseau et à l'environnement physique de l'organisation par les fournisseurs externes doit être surveillé. Les droits d'accès des tiers doivent être périodiquement vérifiés (ex. : mensuellement) et révoqués au besoin.

7.5.7 À l'achat d'un logiciel, l'acheteur devrait demander la liste de l'ensemble des logiciels, des bibliothèques et des systèmes des composants complémentaires. L'entente devrait indiquer les exigences relatives à la mise à jour des éléments des composants.

7.5.8 Les ententes de niveau de service des contrats doivent présenter les exigences et responsabilités des fournisseurs externes relatives au signalement, y compris le délai de signalement acceptable en cas de problème soupçonné.

7.5.9 La prestation de services des fournisseurs externes doit être surveillée pour déterminer s'ils respectent continuellement les exigences opérationnelles et de sécurité qui s'appliquent ainsi que toute exigence du contrat ou de l'entente de niveau de service.

8 Plan et protocoles d'intervention en cas de cyberincident

8.1 Planification

8.1.1 L'organisation doit élaborer, consigner et tenir à jour un plan d'intervention en cas de cyberincident, y compris des plans de continuité des activités et de reprise après sinistre.

8.1.2 Le plan d'intervention en cas de cyberincident peut décrire les étapes d'identification, d'endiguement et d'éradication des menaces et de rétablissement des activités et des systèmes.

8.1.3 Le plan d'intervention en cas de cyberincident doit comprendre des procédures en cas d'interruption des systèmes de soins aux patients et des autres systèmes composées de listes de vérification et de processus manuels ou sur papier pour assurer la continuité et la résilience des activités quotidiennes.

NOTE : Par exemple, un environnement de soins directs aux patients nécessitera des procédures sur papier pour assurer la continuité des tests en laboratoire, de la prise en charge et des transferts de patients, du processus entourant les demandes de médicaments, etc.

8.1.4 Le plan d'intervention en cas de cyberincident, y compris les procédures en cas d'interruption et le plan de reprise après sinistre, est mis à l'essai et validé annuellement.

8.2 Équipe d'intervention en cas d'incident

8.2.1 Le plan d'intervention en cas de cyberincident doit décrire les rôles et les responsabilités pour traiter le cyberincident. L'équipe d'intervention en cas de cyberincident doit être composée, au minimum, d'un gestionnaire d'incident, d'un responsable technique, d'un responsable des ressources humaines, d'un responsable des communications, d'un secrétaire et d'experts en cybersécurité et en protection des renseignements personnels.

8.2.2 L'organisation doit envisager de faire appel à un consultant en intrusion informatique ou à un conseiller juridique qui se spécialise dans les cyberincidents pour aider à gérer les enquêtes, les signalements et les communications en la matière.

8.2.3 L'organisation doit déterminer les activités et services d'intervention en cas de cyberincident qui peuvent être entrepris à l'interne, et ceux qui peuvent être confiés à un tiers.

8.2.4 Le plan d'intervention en cas d'incident de l'organisation doit indiquer les fournisseurs externes de services d'intervention en cas d'incident et de reprise ainsi que les exigences relatives aux services, sous forme d'entente de niveau de service.

8.3 Communication

8.3.1 L'organisation doit élaborer un plan ou un protocole de communication en cas de cyberincident décrivant les stratégies de communication pour les membres de l'équipe d'intervention en cas de cyberincident et pour les parties internes et externes.

8.3.2 Le plan de communication doit présenter les procédures et exigences de signalement pour les professionnels de la santé et le personnel interne et soignant sur place. Il doit aussi indiquer d'autres modes de communication afin que le personnel interne dispose de plusieurs possibilités.

8.3.3 L'organisation doit indiquer et désigner un protocole pour communiquer avec les patients, leur famille, la collectivité, les partenaires et les médias et leur répondre.

8.3.4 L'organisation doit songer à intégrer des modèles d'avis internes et externes dans le plan de communication en cas de cyberincident.

8.4 Communication avec les organismes gouvernementaux de cybersécurité et les organismes d'application de la loi

8.4.1 L'organisation doit disposer d'instructions sur les communications avec les organismes d'application de la loi et les autres organismes gouvernementaux provinciaux, territoriaux et fédéraux qui publient des lignes directrices sur la cybersécurité.

8.4.2 Elle doit signaler aux autorités tout cybercrime comportant un risque même modéré de dommages financiers ou de menace pour la sécurité publique.

8.5 Signalement – Exigences réglementaires et contractuelles

8.5.1 L'organisation doit déterminer et élaborer des procédures pour signaler aux personnes touchées les cyberincidents découlant d'un accès non autorisé à des renseignements personnels (médicaux ou autres) ou de leur divulgation, utilisation ou retrait non autorisés.

8.5.2 Les exigences et procédures de signalement au bureau du commissaire à l'information et à la protection de la vie privée provincial, territorial ou fédéral concerné doivent être élaborées et intégrées au plan d'intervention en cas d'incident.

8.5.3 Les exigences et procédures de signalement aux personnes fichées touchées par les cyberincidents doivent être élaborées et intégrées au plan d'intervention en cas d'incident, conformément aux lois sur la protection de la vie privée qui s'appliquent.

8.5.4 L'organisation doit, s'il y a lieu, disposer de procédures pour intégrer les cyberincidents au Rapport statistique annuel sur les atteintes à la vie privée soumis au commissaire à l'information et à la protection de la vie privée concerné.

8.5.5 Les avis sur les renseignements personnels (médicaux ou autres) doivent comprendre l'information requise par les lois provinciales, territoriales ou fédérales sur la protection de la vie privée qui s'appliquent.

NOTE : Par exemple, les lettres d'avis à une personne touchée par un cyberincident peuvent nécessiter les renseignements suivants : date, heure, durée et description de l'atteinte, description des renseignements touchés, mesures prises pour limiter ou réduire les dommages, mesures prévues pour prévenir les futures atteintes, etc.

8.5.6 L'organisation doit être prête à signaler les cyberincidents à ses partenaires et fournisseurs, aux parties externes et aux fournisseurs de services externes, conformément à ses obligations contractuelles.

8.5.7 Les obligations de signalement des cyberincidents énoncées dans ses différentes ententes contractuelles avec ses partenaires et fournisseurs, les parties externes et les fournisseurs de services externes peuvent être établies et faire l'objet d'un suivi de manière proactive pour répondre aux exigences de signalement.

8.6 Essais et formation

8.6.1 Chaque année, l'organisation doit effectuer des exercices de table et des simulations de cyberincident avec son équipe d'intervention en cas d'incident et ses cadres supérieurs.

8.6.2 L'organisation doit périodiquement mettre à l'essai, passer en revue et réviser ses procédures en cas d'interruption et ses plans d'intervention en cas d'incident, de reprise après sinistre et de communication.

8.6.3 L'organisation doit envisager d'offrir à l'organisme de gouvernance la formation requise sur ses responsabilités de surveillance en cas de cyberincident.

8.7 Assurances

8.7.1 L'organisation devrait envisager de souscrire à une police d'assurance en matière de cybersécurité qui couvre les dommages subis par l'assuré, comme les activités d'intervention, de reprise et d'enquête en cas d'incident, et justifier sa décision de ne pas souscrire à une telle police, le cas échéant.

9 Planification des mesures d'urgence

9.1 Généralités

9.1.1 Lorsque l'organisation déploie une procédure pour les codes d'urgence, elle doit intégrer à la section « Code gris – Défaillance de l'infrastructure essentielle » des procédures d'intervention en cas de défaillance des systèmes de communication, y compris les systèmes téléphoniques et de données.

9.2 Processus manuels et modèles

9.2.1 L'organisation doit se préparer pour un code gris et la défaillance des systèmes de données en élaborant une procédure ou un manuel (possiblement en format papier) pour assurer la sécurité des patients.

NOTE : Par exemple, des formulaires papier disponibles en cas de défaillance des systèmes informatiques d'accueil des patients.

9.2.2 La procédure relative au code gris doit préciser la marche à suivre pour substituer les données une fois que les systèmes sont rétablis.

9.3 Réaffectation de l'effectif

9.3.1 La procédure relative au code gris doit préciser la marche à suivre pour réaffecter l'effectif lorsque les systèmes sont hors service.

9.4 Perte des télécommunications

9.4.1 L'organisation doit se préparer à la perte des systèmes de données en conservant une copie d'urgence des données essentielles et susceptibles de sauver des vies en cas de panne de réseau.

NOTE : Par exemple, l'hôpital B conserve sur un serveur redondant une copie récente des dossiers de patients qui peut être utilisée en mode hors ligne, et la nuit, l'hôpital A imprime les renseignements sur les médicaments des patients.

9.4.2 L'organisation devrait se préparer à la perte des liens de télécommunication en ayant des radios ou des téléphones cellulaires à utiliser en cas de panne.

9.4.3 L'organisation devrait se préparer à la perte des systèmes informatiques en prévoyant des réseaux, des copies de données et des systèmes redondants à haute disponibilité.

9.5 Panne d'électricité pouvant entraîner l'indisponibilité des systèmes informatiques

9.5.1 L'organisation devrait utiliser un système d'alimentation sans coupure (ASC) pour se protéger contre les pannes d'électricité.

NOTE : La gestion d'un tel système peut nécessiter un accès au réseau à des fins de surveillance.

9.5.2 Les procédures d'arrêt d'urgence des systèmes non essentiels doivent être consignées en cas d'instabilité ou de manque de fiabilité de la technologie d'ASC.

9.5.3 L'organisation doit envisager d'instaurer des protocoles d'alimentation électrique redondants afin d'atténuer les risques pour l'infrastructure de gestion de l'alimentation qui menacent directement la sûreté et la disponibilité des soins. Les petites organisations sans dispositifs essentiels peuvent se contenter d'un système d'ASC, mais les plus grosses doivent se doter de mécanismes de cybersécurité des TO pour protéger ladite infrastructure vitale.

9.6 Perte des technologies de soins virtuels

9.6.1 Les procédures d'urgence de l'organisation doivent comprendre un plan de continuité des soins pour les patients qui ne reçoivent pas de soins en personne. Par exemple, ces patients peuvent utiliser des solutions de télésurveillance ou de consultation virtuelle.

10 Surveillance et mesure

10.1 Surveillance

10.1.1 L'organisation doit déployer les processus requis pour journaliser, détecter et examiner les activités anormales et pour surveiller les cyberactivités liées aux environnements de TO et de TI, y compris ce qui suit :

a. Recueillir et conserver les journaux requis des systèmes, des pare-feu, des réseaux et des événements.

b. Établir les activités de base des systèmes, des réseaux et des canaux de communication.

c. Établir un processus pour rapprocher les données recueillies afin de cerner les activités anormales potentielles.

d. Établir les degrés de gravité et de priorité des activités anormales recensées;

e. Déterminer le seuil de lancement d'une intervention officielle en cas de cyberincident.

10.1.2 L'organisation doit envisager de déployer un processus continu de surveillance des incidents et des événements de sécurité pour détecter les cyberincidents rapidement et, dans la mesure du possible, mettre en place des systèmes d'alerte automatique en cas d'activités anormales.

10.1.3 L'organisation doit diviser ses actifs de TI et de TO en fonction de leur importance et de l'utilisation qui en est faite afin de séparer le réseau et l'équipement employés dans les soins aux patients des systèmes opérationnels.

10.1.4 L'organisation doit surveiller et évaluer les répercussions des vulnérabilités du jour zéro qui peuvent être exploitées par les cybercriminels et suivre les recommandations requises du fournisseur pour y remédier rapidement.

10.2 Tests d'intrusion

10.2.1 L'organisation doit envisager de réaliser périodiquement des tests d'intrusion pour recenser les vulnérabilités potentielles et assurer l'efficacité de ses processus de gestion des vulnérabilités.

NOTE : Différents types de tests d'intrusion et d'évaluations des vulnérabilités sont à la disposition des organisations : tests d'intrusion internes, externes, des applications Web et du réseau sans fil, évaluation de la configuration, etc.

10.2.2 S'il y a lieu, l'organisation doit réaliser des évaluations des cyberrisques et des vulnérabilités ainsi que des tests d'intrusion axés sur les TO.

NOTE : Certains actifs de TO peuvent être mis hors service par les tests d'intrusion et les balayages des vulnérabilités. On leur accordera donc une attention particulière afin d'éviter les problèmes.

L'approche adoptée pour ces essais dans les environnements de TO devrait être responsable et prudente, puisque les conséquences d'une panne pourraient être graves. Les méthodes sont différentes dans ces environnements en raison des particularités des TO. Par exemple, les appareils d'IRM, de radiographie et de dialyse ne peuvent être mis à l'essai de la même façon qu'un appareil de TI standard.

10.3 Exercice de l'équipe rouge contre l'équipe bleue

10.3.1 L'organisation doit envisager d'effectuer des exercices de simulation avec une équipe rouge et une équipe bleue pour former le personnel à reconnaître et à contrer les attaques ciblées.

10.4 Chasse aux menaces

10.4.1 L'organisation doit envisager de mener des activités de manière proactive pour trouver les cybermenaces non détectées dans son environnement.

10.4.2 Les activités de chasse aux menaces peuvent s'appuyer sur des connaissances continuellement tirées de différentes activités de cyberrenseignement nationales et internationales, y compris les tactiques d'attaques connues et les indicateurs de compromission.

10.4.3 L'organisation devrait participer à des groupes d'échange d'information pour demeurer à l'affût des cybermenaces émergentes, améliorer sa capacité à intervenir et accroître sa résilience.

Annexe A
(Informative)

A. Pourquoi les organisations de santé sont-elles de si grosses cibles?

Pour assurer un soutien direct et indirect à leurs patients, les organisations de santé utilisent un grand nombre de technologies et de dispositifs. Or, les environnements et les dispositifs technologiques en santé ne sont pas toujours très bien sécurisés, et les organisations omettent souvent d'appliquer les correctifs ou de faire les mises à jour, à cause de facteurs complexes comme le manque de ressources, les dépendances et interdépendances des systèmes, et les répercussions néfastes de l'indisponibilité prolongée d'un système. Sans compter que le manque de financement relègue souvent au second plan les investissements dans les contrôles et processus de cybersécurité.

Par ailleurs, l'évolution constante des menaces augmente les risques de cyberattaque par compromission de la chaîne d'approvisionnement ou intrusion dans les technologies opérationnelles (TO) et les systèmes de contrôle industriel (SCI).

Ainsi, entre les infrastructures obsolètes et vulnérables et le personnel susceptible à l'exploitation et au piratage, les organisations de santé sont particulièrement exposées, d'autant plus qu'elles sont souvent ouvertes à négocier et à collaborer avec les cybercriminels pour remettre leurs systèmes en état et éviter les atteintes à la vie privée.

Pourquoi les cybercriminels aiment-ils tant les renseignements médicaux personnels?
Les renseignements médicaux personnels sont considérés comme les renseignements les plus sensibles et à risque d'une personne, plus que ses cartes de crédit et ses renseignements bancaires. Les organisations de santé recueillent et stockent d'immenses quantités de renseignements médicaux et de données sensibles dont le vol ou l'altération pourrait porter préjudice aux patients. S'il est possible de gérer le vol ou la perte de données financières (ex. : prévention des fraudes), il n'existe pas de façon de récupérer, de changer ou de remplacer des renseignements médicaux volés ou perdus.

Les cybercriminels peuvent se servir de ces renseignements de plusieurs façons :

- Chiffrer les données et restreindre l'accès aux systèmes essentiels, puis demander une rançon en échange de la clé de déchiffrement qui permettra à l'organisation de reprendre le contrôle sur ses systèmes.

- Voler des renseignements médicaux personnels et de l'information sensible et extorquer de l'argent à l'organisation de santé en menaçant de divulguer le tout ou en promettant de supprimer les données volées.

- Vendre sur le Web clandestin des ensembles de renseignements médicaux et financiers, avec lesquels on peut créer de fausses identités

Annexe B
(Informative)

B. Étude de cas

Voici une étude de cas décrivant une cyberattaque et les enjeux liés à la gestion de la brèche de sécurité. Elle vise à informer le lecteur des risques, des répercussions et des coûts qui peuvent découler d'une attaque.

Cyberattaque :

Vecteur d'attaque initial

Un membre du personnel administratif a reçu un courriel d'hameçonnage accompagné d'un document malveillant contenant une macro. Lorsqu'il a ouvert le document, la macro a installé plusieurs maliciels, dont un rançongiciel connu pour chiffrer et voler les données.

Les données de plusieurs serveurs ont alors été chiffrées ou corrompues, ce qui a nui aux activités cliniques de l'organisation. De multiples systèmes documentaires sont passés en mode manuel, et d'autres organisations ont dû prendre la relève des services. Les communications par courriel et par téléphone ont aussi brièvement cessé en raison d'une perte de l'accès Internet.

Heureusement, les copies de sauvegarde étaient intactes. Les pirates demandaient une rançon en échange de la clé et des instructions de déchiffrement, mais l'organisation a décidé de ne pas payer et a pu restaurer ses systèmes à partir d'une sauvegarde.

Deuxième vague

Quelques jours après la restauration des systèmes, les pirates à l'origine de l'attaque par maliciels ont envoyé un courriel à plusieurs adresses de l'organisation, promettant de supprimer les données volées en échange d'un million de dollars américains. L'organisation de santé a fait appel à une entreprise de criminologie pour enquêter sur la possibilité d'un vol de données. L'enquête a révélé une extraction de données de plusieurs serveurs. L'organisation a donc embauché une société pour demander aux pirates une preuve du vol, qui a été fournie. La décision a finalement été prise de payer la rançon pour que les données soient supprimées.

Suivant des échanges entre un consultant en intrusion, les pirates, l'entreprise de criminologie et un négociateur, la rançon a été abaissée à 300 000 dollars américains. Une fois le total payé, les pirates ont envoyé une confirmation que les données avaient été supprimées. L'organisation de santé a ensuite entrepris un processus d'investigation électronique pour déterminer quels renseignements avaient été obtenus.

Le bureau du commissaire à l'information et à la protection de la vie privée régional a aussi été avisé de l'attaque par rançongiciel et du vol de données.

Considérations importantes

1. Communication

L'organisation de santé a avisé les parties assurées dans les heures suivant la découverte des anomalies dans son système. Avec l'aide de son conseiller juridique, d'un consultant externe en intrusion informatique, de son assureur et de son service des relations avec les médias et des communications, elle a notifié son conseil d'administration, ses partenaires et la communauté. Son personnel a été informé selon la structure de sortance en place, conformément au système de gestion des incidents. Elle a aussi mis à jour son site Web pour aviser le public de la période d'indisponibilité imprévue et de l'état des services.

Enfin, elle a préparé avec le consultant externe plusieurs textes pour répondre aux questions des intervenants, des partenaires, des patients, des familles et des médias.

2. Répercussions cliniques

L'organisation de santé utilisait un système centralisé de saisie des ordonnances. Lorsque celui-ci a été mis hors service, elle a dû retourner aux ordonnances papier pour les traitements, les médicaments, les admissions et sorties, les analyses de laboratoire, l'imagerie diagnostique, etc. Cela a entraîné des retards dans la transmission des renseignements cliniques aux différents acteurs (cercle de soins, autres établissements, etc.). Les processus de gestion des médicaments (commandes, dispensation, inventaire des substances de contrôle, restockage, gestion des demandes urgentes, etc.) ont aussi dû être réalisés entièrement manuellement. En attendant le retour des systèmes, des mesures supplémentaires ont été prises pour vérifier et corriger les problèmes dans les soins et les données inexactes.

3. Correction et reprise

L'organisation utilisait environ 3 500 terminaux et 300 serveurs physiques et virtuels, tous connectés au même réseau opérationnel. Lorsqu'elle a été attaquée, elle craignait que le réseau tout entier ait été compromis. Plusieurs fournisseurs de cybersécurité ont été appelés en renfort pour trouver, isoler et retirer les maliciels. Les serveurs et les terminaux ont été restaurés à partir de copies de sauvegarde et d'images.

Des mécanismes de sécurité supplémentaires ont ensuite été mis en place pour assurer la surveillance des terminaux et le blocage ou la mise en quarantaine de tout autre maliciel éventuel. L'organisation a aussi amélioré ses filtres courriel et Web, déployé l'authentification multifacteur à grande échelle, divisé et segmenté ses réseaux et resserré la sécurité de son pare-feu. Enfin, elle a changé tous les mots de passe de ses utilisateurs.

4. Coûts d'une attaque

Voici les dépenses encourues par l'organisation de santé à la suite de l'attaque par rançongiciel. Le total s'élevait approximativement à cinq millions de dollars canadiens :

- Paiement de la rançon (300 000 $ US)
- Confinement du rançongiciel
- Rétablissement des systèmes à partir des sauvegardes
- Enquête judiciaire par un tiers
- Acquisition de logiciels pour la détection des intrusions

- Acquisition de logiciels pour le confinement et la rectification
- Données cellulaires utilisées pendant la panne
- Frais des consultations juridiques et en intrusion informatique
- Autres services professionnels (consultants en intrusion informatique, consultants en cybersécurité)
- Communications avec les patients, les autorités de réglementation, la communauté, les partenaires et les intervenants
- Matériel supplémentaire (ex. : remplacement de vieux serveurs inutilisables)
- Heures supplémentaires du personnel informatique
- Heures pour la récupération des données (ex. : saisie manuelle)
- Heures supplémentaires du personnel de bureau pendant la panne
- Personnel clinique supplémentaire pour les soins aux patients (ex. : pour réduire l'attente)
- Pertes de revenus liées à la redirection des soins
- Coûts en capital du matériel, des logiciels et du soutien continu (ex. : pare-feu, authentification multifacteur, VPN, détection et intervention aux terminaux)
- Fournisseurs de services informatiques pour la restauration des systèmes et des données

Annexe C
(informative)

C. Modèle de plan d'intervention en cas d'incident

Note : Ce modèle provient de la norme CAN/CIOSC 104:2021.

C.1 Portée

C.1.1 Le présent plan d'intervention en cas d'incident s'applique à l'ensemble des réseaux, systèmes, données et membres de l'organisation, y compris tout employé, entrepreneur et fournisseur qui accède à ces réseaux, systèmes et données. Les membres de l'organisation qui peuvent avoir à diriger l'équipe d'intervention en cas d'incident ou à en faire partie doivent prendre connaissance de ce plan et se préparer à collaborer en vue de réduire au minimum les conséquences des incidents sur l'organisation.

C.1.2 Le présent plan constitue pour l'organisation un moyen d'établir ses capacités de traitement des incidents et d'intervention, ainsi que les mesures à prendre en réponse aux incidents de sécurité courants.

C.2 Exigences

C.2.1 Tout employé, entrepreneur, consultant, salarié temporaire ou autre membre de l'organisation et de ses filiales qui se rend compte d'une anomalie mettant en cause les données ou de la possibilité d'un incident de cybersécurité doit immédiatement en informer son superviseur et le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation.

C.2.2 Les renseignements suivants sont notés lors du signalement d'un incident de sécurité réel ou potentiel (ex. : intrusion) :

a. Déroulement de l'incident

b. Endroit de l'incident (ex. : service de l'organisation)

c. Moment de l'incident

d. Manière et moment de la découverte de l'incident

e. Type d'incident (si connu)

f. Équipement ou partie de l'environnement de TI touché

g. Mesures correctives prises (le cas échéant)

C.2.3 Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation examine les circonstances de l'incident réel ou potentiel, lequel est signalé dès sa découverte, et les renseignements ci-dessus sont consignés.

C.2.4 L'organisation enquête sur tout signalement d'incident de sécurité en suivant les étapes standard (préparation, identification, endiguement, éradication, reprise, bilan) ou un processus

équivalent (ci-après, « le processus de gestion des incidents de sécurité »).

a. Préparation

i. L'organisation conserve une version papier du plan d'intervention en cas d'incident, en plus de sa version numérique, pour en assurer l'accessibilité quel que soit l'état de l'infrastructure de TI interne.

NOTE : La politique de conservation de l'organisation prévoit des exigences et des obligations concernant la conservation des documents et des dossiers et les contrôles de vérification.

ii. Le plan d'intervention en cas d'incident est révisé chaque année et après chaque incident.

iii. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation établit à l'avance la composition de l'équipe requise pour mettre en œuvre le processus de gestion des incidents de sécurité (ci-après, « l'équipe d'intervention en cas d'incident de sécurité »).

iv. La composition de l'équipe d'intervention en cas d'incident de sécurité est indiquée dans le plan d'intervention en cas d'incident.

v. Tout employé, entrepreneur, consultant, travailleur temporaire ou autre membre de l'organisation, y compris les membres de l'équipe d'intervention en cas d'incident de sécurité, est formé convenablement de sorte qu'il comprenne le processus de gestion des incidents de sécurité et le rôle qu'il a à y jouer.

vi. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation organise des exercices de formation annuels sur les incidents de sécurité en collaboration avec l'équipe d'intervention en cas d'incident de sécurité.

NOTE : Ces exercices permettent à l'équipe d'intervention en cas d'incident de sécurité d'acquérir une connaissance préalable des types d'incidents et d'être prête à répondre aux éléments connus de sorte à pouvoir se concentrer sur les éléments inconnus, et de mettre à l'essai de manière exhaustive le plan, l'équipe et les outils.

vii. Les documents sur l'environnement de TI de l'organisation (renseignements de référence, sur les dépendances et sur les fournisseurs) sont tenus à jour et accessibles en tout temps.

b. Identification

i. Tout employé, entrepreneur, consultant, travailleur temporaire ou autre membre de l'organisation, y compris les membres de l'équipe d'intervention en cas d'incident de sécurité, se renseigne sur les types d'incidents de sécurité suivants :

- Utilisation ou accès non autorisé
- Interruption ou déni de service
- Code malveillant
- Défaillance du réseau (généralisée)
- Défaillance du système d'applications
- Divulgation non autorisée ou perte d'information
- Atteinte à la vie privée
- Atteinte aux données ou à la sécurité de l'information
- Autre (tout autre incident touchant les réseaux, systèmes ou données)

ii. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation détermine la gravité (voir le tableau 1) de l'incident selon les facteurs suivants : nombre de systèmes touchés, caractère essentiel des systèmes touchés, nombre de personnes et d'équipes touchées (jusqu'à la totalité de l'organisation), nombre de secteurs d'activité touchés et conséquences de l'incident. Il examine le contexte opérationnel pertinent et les autres activités en cours de l'organisation pour bien comprendre les conséquences et l'urgence de la prise de mesures correctives.

iii. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation examine l'information disponible pour déterminer l'importance connue des conséquences et la comparer à son ampleur estimée en tenant compte de la possibilité et de la rapidité de propagation. Il évalue les conséquences potentielles pour l'organisation sur le plan des finances, de la marque, de la réputation, etc.

NOTE : L'incident de sécurité peut résulter d'une menace simple ou sophistiquée ou d'une attaque automatisée ou manuelle, ou être un acte de nuisance ou de vandalisme.

iv. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation détermine s'il y a présence d'une vulnérabilité et d'un exploit, si des signes révèlent quelle vulnérabilité est exploitée et s'il existe un correctif. Il détermine aussi s'il s'agit d'une nouvelle menace (du jour zéro) ou d'une menace connue, et estime le travail d'endiguement requis.

Catégorie	Indicateurs	Portée
1 – Critique	Perte de données, maliciel	Généralisée, serveurs critiques ou fuite de données
2 – Élevé	Menace théorique devenue active	Généralisée, serveurs critiques ou fuite de données
3 – Modéré	Hameçonnage par courriel ou infection active en propagation	Généralisée
4 – Faible	Maliciel ou hameçonnage	Un seul hôte ou une seule personne

Tableau 1 : Gravité des incidents

v. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation prépare un plan de communication en cas d'incident de sécurité afin que soient facilement accessibles les coordonnées du personnel de l'organisation, de l'équipe d'intervention en cas d'incident de sécurité et des tierces parties pertinentes, comme la compagnie d'assurance en matière de cybersécurité.

vi. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation évalue la situation et détermine s'il y a eu atteinte à la vie privée en répondant aux deux questions suivantes :

- **L'incident touche-t-il des renseignements personnels identificatoires?** Pour vérifier s'il y a atteinte à la vie privée, il faut déterminer le type de renseignements touchés par l'incident.

- **Y a-t-il eu divulgation non autorisée?** Qu'elle ait été intentionnelle, involontaire ou de nature criminelle, une divulgation non autorisée constitue une atteinte à la vie privée.

  NOTE 1 : Si la réponse aux deux questions est « oui », il y a eu atteinte à la vie privée.

  NOTE 2 : S'il y a eu atteinte à la vie privée, l'organisation peut être tenue de le signaler à l'autorité compétente.

vii. Ayant déterminé le type et la gravité de l'incident et s'il y a eu atteinte à la vie privée, le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation est en mesure de confirmer si un incident de sécurité s'est produit. Le cas échéant, les étapes suivantes du plan d'intervention en cas d'incident sont effectuées.

viii. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation réunit immédiatement l'équipe d'intervention en cas

d’incident de sécurité pour préciser la nature de l’incident et recueillir des données à son sujet.

ix. L’équipe d’intervention en cas d’incident de sécurité établit la priorité de l’incident et consigne l’information recueillie et les décisions, notamment :

- le signalement initial, le type et la gravité de l’incident, la détermination concernant l’atteinte à la vie privée, et les mesures prises;
- l’analyse des précurseurs et des indicateurs;
- les incidents de sécurité connus apparemment semblables;
- tout acteur, mécanisme, application, vecteur d’attaque possible et tout autre renseignement facilitant l’endiguement et l’éradication de la cause profonde de l’incident.

c. Endiguement

i. L’équipe d’intervention en cas d’incident de sécurité consigne tout renseignement obtenu et toute mesure prise durant l’endiguement de l’incident, qui comprend les interventions suivantes :

- Circonscrire immédiatement l’incident, dans la mesure du possible, en isolant l’infrastructure touchée.
- Déterminer la source de l’incident, notamment la vulnérabilité exploitée.
- Corriger immédiatement toute vulnérabilité cernée ou mettre en place des solutions de contournement pour pallier les systèmes touchés.
- Évaluer en continu les conséquences et les préjudices, et confirmer la portée de l’incident.
- Déterminer les changements de l’environnement (fichiers, connexions, processus, comptes, accès, etc.).
- Obtenir, conserver, mettre en sécurité et consigner les preuves, et préserver la chaîne de possession.

d. Éradication

i. L’équipe d’intervention en cas d’incident de sécurité consigne tout renseignement obtenu et toute mesure prise durant l’éradication des conséquences de l’incident, qui comprend les interventions suivantes :

- Éliminer toute trace de l’incident.

- Déterminer et atténuer les vulnérabilités relevées durant l'enquête, qu'elles aient été exploitées ou non lors de l'incident.
- Éliminer le maliciel, le virus, le matériel inapproprié et tout autre élément introduit pendant l'incident. Au besoin, suivre les processus de restauration de la sauvegarde pour assurer l'absence de code malveillant dans l'environnement.
- S'il y a découverte d'autres appareils touchés dans l'environnement, reprendre les étapes d'identification et d'endiguement pour ces appareils.
- Poursuivre les recherches et l'enquête jusqu'à ce que l'ensemble du vecteur d'attaque soit compris.
- Enfin, prendre les mesures nécessaires pour empêcher la récurrence de l'incident.

e. Reprise

i. L'équipe d'intervention en cas d'incident de sécurité consigne tout renseignement obtenu et toute mesure prise durant la reprise après l'incident, qui comprend les interventions suivantes :

- Ramener un à un les systèmes touchés à l'état opérationnel de manière à rétablir le fonctionnement en limitant le risque de récurrence de l'incident.
- Surveiller étroitement chaque système remis en service ainsi que tout appareil en périphérie du réseau pour s'assurer que l'incident ne se reproduira pas ou n'est pas encore en cours.
- Veiller à restaurer les systèmes à partir d'une source de confiance non infectée.
- Vérifier que les systèmes touchés fonctionnent normalement.
- Mettre en place une surveillance supplémentaire pour repérer toute activité future associée à l'incident, au besoin.

f. Bilan

i. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation est chargé de produire un rapport de suivi sur l'incident de sécurité.

ii. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation organise une réunion avec l'équipe d'intervention en cas d'incident dans les deux semaines pour faire le bilan de l'incident et passer en

revue le rapport produit. Cette réunion devrait donner lieu, entre autres, aux résultats suivants :

- Analyse détaillée du déroulement de l'incident décrit dans le rapport
- Description des circonstances de la découverte de l'incident (comment, quand, par qui)
- Description de la portée et de la gravité de l'incident
- Analyse des méthodes d'endiguement et d'éradication de l'incident
- Détermination des améliorations possibles en prévision d'incidents futurs
- Attribution des responsabilités relatives au suivi de ces améliorations

iii. Les résultats de la réunion sont consignés et conservés avec les documents sur l'incident de sécurité.

Annexe D
(informative)

D. Questionnaire d'évaluation des risques de cybersécurité

Le questionnaire d'évaluation des risques de cybersécurité ci-dessous vise à sensibiliser les organisations de santé. Il ne sert pas à porter un jugement ou à produire une cote de risque globale. Le membre de l'équipe de direction nommé à la surveillance de la sécurité des TI de l'organisation devrait demander à des experts en cybersécurité d'examiner et de commenter son évaluation des risques et le choix des contrôles visant à protéger l'organisation contre les risques cernés et évalués. Aux fins du présent document, on entend par « politique » les règles et les procédures que doit suivre toute personne utilisant un actif ou une ressource informatique de l'organisation. La réponse « non » à l'une des questions pourrait indiquer l'existence d'un risque pour l'organisation.

1. Les rôles et responsabilités relatifs aux TI et à la sécurité des TI sont-ils clairement définis dans votre organisation?	OUI / NON
2. Votre organisation a-t-elle un plan d'intervention en cas d'incident? 2a. Les actifs de TO (appareils de radiographie, de dialyse, de surveillance des patients, etc.) sont-ils couverts par un tel plan?	OUI / NON OUI / NON
3. Votre organisation a-t-elle une assurance en matière de cybersécurité? 3a. Le cas échéant, celle-ci couvre-t-elle les actifs de TO de l'organisation?	OUI / NON OUI / NON
4. Votre organisation a-t-elle évalué le préjudice potentiel lié à la confidentialité, à l'intégrité et à l'accessibilité de ses actifs et systèmes d'information? https://lh-ca.cyber.gc.ca/login/index.php?lang=fr_ca	OUI / NON
5. Votre organisation stocke-t-elle ou recueille-t-elle des données confidentielles (numéros de cartes de crédit ou de sécurité sociale, renseignements sur les employés, etc.)?	OUI / NON
6. Votre organisation connaît-elle ses responsabilités en vertu de la *Loi sur la protection des renseignements personnels*? https://laws-lois.justice.gc.ca/fra/lois/P-21/index.html	OUI / NON
7. Votre organisation a-t-elle classifié les données stockées?	OUI / NON
8. Votre organisation forme-t-elle ses employés sur ses politiques et procédures de cybersécurité?	OUI / NON
9. Votre organisation a-t-elle une politique interne établissant les dépenses en cybersécurité en fonction du budget total des TI?	OUI / NON
10. Votre organisation forme-t-elle son personnel des TI sur la cybersécurité?	OUI / NON

11. L'application automatique de correctifs est-elle activée partout où elle peut l'être?	OUI / NON
12. Votre organisation a-t-elle une politique sur la sauvegarde et le chiffrement des données opérationnelles essentielles?	OUI / NON
13. Votre organisation a-t-elle une politique sur l'emploi d'une authentification robuste des utilisateurs?	OUI / NON
14. Votre organisation a-t-elle une politique sur l'autorisation et le contrôle de l'accès?	OUI / NON
15. Votre organisation a-t-elle une politique sur la sécurité des sites Web?	OUI / NON
16. Votre organisation a-t-elle une politique sur la sécurité des services mobiles?	OUI / NON
17. Votre organisation a-t-elle une politique sur l'établissement de défenses de base sur le périmètre? 17a. A-t-elle une politique pour assurer la segmentation des protocoles pare-feu pour les réseaux de TI et de TO?	OUI / NON OUI / NON
18. Votre organisation a-t-elle recours à des services de TI de tiers (ex. : services infonuagiques, logiciels à la demande, sauvegarde à distance)?	OUI / NON
19. Votre organisation a-t-elle une politique sur les services de TI de tiers?	OUI / NON
20. Votre organisation vérifie-t-elle les contrôles de sécurité en vigueur au moins une fois par année?	OUI / NON
21. Votre organisation soumet-elle ses systèmes d'information et ses actifs de TO à des essais de pénétration et de vulnérabilité au moins une fois par année?	OUI / NON

Annexe E
(informative)

E. Matrice RACI

Dans un programme de sécurité efficace, chaque personne a un rôle à jouer et les responsabilités de chacun relatives à la sécurité sont clairement définies. Si les énoncés de politique généraux demeurent importants, des renseignements supplémentaires sur les rôles et responsabilités peuvent être présentés dans une matrice RACI pour préciser les responsables (poste ou équipe) de chaque aspect de la sécurité.

Dans les petites organisations, la répartition des tâches peut poser problème, puisqu'une même personne doit parfois jouer plusieurs rôles. Dans ce cas, il demeure possible d'appliquer le principe autrement, en gardant une deuxième personne au courant des activités essentielles, par exemple :

- Surveillance et signalement des actions des administrateurs (ex. : envoi d'alertes au gestionnaire lorsque le responsable des TI se connecte à des comptes administrateur);
- Évaluations par les pairs et approbations des changements à la production.

La matrice RACI (responsable, approbateur, consulté, informé) sert à décrire et à attribuer clairement les différentes fonctions relatives à la sécurité dans l'organisation.

Voici les définitions des éléments de la matrice RACI :

Terme	Définition	Question à se poser
Responsable	Personne ou équipe qui doit effectuer la tâche ou déployer le contrôle, notamment en soutenant ou en mettant en œuvre la solution.	Qui effectue la tâche?
Approbateur	Personne assumant la responsabilité ultime d'un sujet, d'un processus ou d'une portée. Elle est responsable de la réussite de la tâche ou du contrôle de sécurité et détermine si le déploiement du contrôle de sécurité a donné les résultats escomptés.	Qui est responsable du résultat de la tâche?
Consulté	Personne ou équipe dont l'avis sur une activité est sollicité (communication bidirectionnelle). Ce sont les principales personnes et équipes qui soumettent des commentaires. À noter qu'il incombe à l'approbateur et au responsable d'obtenir de l'information sur tout autre groupe concerné, mais les commentaires des personnes et équipes consultées doivent être pris en compte et, au besoin, faire l'objet de mesures.	Qui fournit un avis?
Informé	Personne qui est tenue au courant du progrès d'une activité (communication unidirectionnelle). Les personnes informées n'approuvent rien, mais sont informées des résultats ou des livrables de la tâche. Elles doivent être tenues au courant du	Qui reçoit l'information sur la

	progrès des activités, mais ne sont pas informées des détails et ne participent pas aux activités en cours. À noter que les responsables et les approbateurs doivent aussi être informés.	tâche et les résultats?

Les rôles indiqués dans l'en-tête, les activités de la première colonne et le modèle rempli sont fournis à titre d'exemple seulement. Chaque organisation est unique et, à des fins de clarté, il importe que les rôles soient associés aux équipes et services correspondants de votre organisation.

Chaque équipe comprise dans la matrice RACI doit pouvoir examiner, comprendre et approuver leurs activités liées à la sécurité de l'information de l'organisation. Voici un exemple de matrice RACI :

Activité	**RSSI**	**Équipe de sécurité**	**Soutien des branches d'activité**	**Service de TI/d'assistance**	**Équipe de direction**
Stratégie de sécurité	A	R	C	C	I
Planifier l'actualisation des systèmes d'information et de l'infrastructure.	I	I		A/R	C
Évaluation des risques de sécurité	A	R	A (R)	C/I	
Évaluer les menaces et les risques, au besoin.	A	R	C	R	R
Veiller à l'approbation rapide et adéquate des exceptions aux politiques, des risques et des plans d'atténuation des risques liés à la sécurité de l'information.	I	C	R	I	A
Faire le suivi de l'état des risques de sécurité actifs et en faire rapport à l'équipe de direction ou de gestion.	A	R	C/I	C/I	I

Dans les en-têtes de colonne, inscrivez tout groupe qui joue un rôle dans la gestion de la sécurité de l'organisation, y compris les branches d'activités et les fournisseurs de services gérés et de services de sécurité gérés.

La liste non exhaustive ci-dessous peut servir de guide pour les activités à ajouter à la matrice RACI.

- Stratégie de sécurité
    - Planifier l'actualisation des systèmes d'information et de l'infrastructure.
- Évaluation des risques de sécurité
    - Évaluer les menaces et les risques, au besoin.
    - Veiller à l'approbation rapide et adéquate des exceptions aux politiques, des risques et des plans d'atténuation des risques liés à la sécurité de l'information.

- Faire le suivi de l’état des risques de sécurité actifs et en faire rapport à l’équipe de direction ou de gestion.

- Sensibilisation et formation sur la sécurité
  - Élaborer, gérer et offrir une formation annuelle sur la protection de la vie privée et la sécurité.
  - Offrir des formations et du mentorat sur le développement sécuritaire adaptés aux rôles.
  - Offrir aux autres parties (utilisateurs privilégiés, services des finances et des ressources humaines, etc.) des formations adaptées aux rôles.
  - Former les nouveaux employés.
- Exercices d’hameçonnage
  - Veiller à la conformité aux exigences de formation sur la sécurité.
- Politiques de sécurité
- Intervention en cas d’incident de sécurité
  - Gestion des problèmes liés à la sécurité de l’information, les incidents et les atteintes, y compris la gestion des incidents de sécurité.
  - Soutien de premier niveau.
  - Intervention externe en cas d’incident (service d’assistance de la branche d’activités) – Premier appel, tri.
  - Intervention interne en cas d’incident (service d’assistance des TI) – Premier appel, tri.
  - Processus de résolution des problèmes – Responsable de la sécurité.
  - Entente sur les niveaux de service des tiers pour les interventions en cas d’incident.
  - Lancement du processus de demande d’indemnisation.
- Architecture de sécurité
  - Trouver et choisir les solutions de sécurité.
  - Approuver les solutions de sécurité.
  - Établir la feuille de route pour la mise en œuvre des solutions de sécurité.
  - Mettre en œuvre la feuille de route sur la sécurité.
  - Fournir les accès aux outils de sécurité.

- Veiller à ce que les nouveaux systèmes soient compatibles avec les outils de sécurité.
- Établir des indicateurs pour les rapports sur la sécurité.

- Sécurité des applications
  - Test de sécurité interne.
  - Test de sécurité externe.
- Sécurité de l'infrastructure
  - Configurer les appareils de façon à ce qu'ils soient sécuritaires.
- Activités de sécurité
  - Disposer de processus de surveillance et de détection pour assurer la sécurité de l'information.
  - Analyser et, au besoin, rapprocher les journaux pour détecter les atteintes potentielles à la sécurité de l'information.
  - Appliquer des correctifs de sécurité dans les délais établis.
  - Gérer les certificats numériques et l'enregistrement de domaines.
  - Exploiter et surveiller des antivirus et des solutions antimaliciels.
  - Déployer et surveiller des contrôles de sécurité des terminaux (y compris la détection des menaces et l'intervention aux terminaux).
  - Fonctions de sauvegarde et de restauration (sur place, dans le nuage).
- Sécurité réseau
  - Offrir des services de sécurité conformes aux définitions (dans l'architecture de sécurité).
  - Configurer les pare-feu, les routeurs, les commutateurs et les réseaux sans fil.
  - Modifier les pare-feu, les routeurs, les commutateurs et les réseaux sans fil.
  - Configurer l'infrastructure et l'infrastructure infonuagique.
  - Diviser les réseaux de TI et de TO.
- Gestion des vulnérabilités
  - Analyser les vulnérabilités.
  - Remédier aux vulnérabilités dans les délais convenus.
  - Réaliser des tests d'intrusion.

- Conformité réglementaire
    - Veiller à ce que les contrôles de sécurité soient conformes aux objectifs de l'entreprise et à la réglementation.
    - Surveiller la conformité aux contrôles de sécurité.
    - Surveiller la conformité des fournisseurs aux contrôles de sécurité.
- Cycle de vie des employés
    - Vérifications des antécédents.
    - Ajout, modification et déplacement d'employés.
- Approvisionnement
    - Évaluations des nouveaux fournisseurs.
    - Évaluation des risques de sécurité des fournisseurs.
    - Clauses de sécurité dans les contrats.

Bibliographie

[1]. CAN/CIOSC 103-1, *Confiance et identité numérique – Partie 1 : Notions fondamentales*.

[2]. Centre canadien pour la cybersécurité. *Contrôles de cybersécurité de base pour les petites et moyennes organisations*.

[3]. Cyber Essentials, Royaume-Uni.

[4]. Cyber Essentials, Nouveau-Brunswick.

[5]. *Post market Management of Cybersecurity in Medical Devices* https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

[6]. IEC TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*.

[7]. ISACA. *Cybersecurity Guidance for Small and Medium-sized Enterprises*, 2015.

[8]. ISACA. *Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises*, 2015.

[9]. ISO 19731:2017, *Analytique numérique et analyses web pour les besoins d'études de marché, études sociales et d'opinion – Vocabulaire et exigences de service*.

[10]. ISO/IEC 27032:2012, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité*.

[11]. ISO/IEC 27000:2018, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*.

[12]. ISO/IEC 27001:2013, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*.

[13]. ISO/IEC 27002:2013, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*.

[14]. ITSAP.30.032, *Pratiques exemplaires de création de phrases de passe et de mots de passe*.

[15]. Open Web Application Security Project. *Application Security Verification Standard*.

[16]. Open Web Application Security Project. *Top 10 Vulnerabilities*.

[17]. National Institute of Standards and Technology (NIST). *Cyber Security Framework*.

[18]. Industrie des cartes de paiement. *Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)*.

[19]. IASME. *Governance Standard for Information and Cyber Security*.