Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information

Institut canadien d'information sur la santé
Canadian Institute for Health Information

La production du présent document est rendue possible grâce à un apport financier de Santé Canada et des gouvernements provinciaux et territoriaux. Les opinions exprimées dans ce rapport ne représentent pas nécessairement celles de Santé Canada ou celles des gouvernements provinciaux et territoriaux.

À moins d'indication contraire, les données utilisées proviennent des provinces et territoires du Canada.

Tous droits réservés.

Le contenu de cette publication peut être reproduit tel quel, en tout ou en partie et par quelque moyen que ce soit, uniquement à des fins non commerciales pourvu que l'Institut canadien d'information sur la santé soit clairement identifié comme le titulaire du droit d'auteur. Toute reproduction ou utilisation de cette publication et de son contenu à des fins commerciales requiert l'autorisation écrite préalable de l'Institut canadien d'information sur la santé. La reproduction ou l'utilisation de cette publication ou de son contenu qui sous-entend le consentement de l'Institut canadien d'information sur la santé, ou toute affiliation avec celui-ci, est interdite.

Pour obtenir une autorisation ou des renseignements, veuillez contacter l'ICIS :

Institut canadien d'information sur la santé
495, chemin Richmond, bureau 600
Ottawa (Ontario) K2A 4H6
Téléphone : 613-241-7860
Télécopieur : 613-241-8120
icis.ca
droitdauteur@icis.ca

© 2022 Institut canadien d'information sur la santé

Comment citer ce document :
Institut canadien d'information sur la santé. *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information*. Ottawa, ON : ICIS; 2022.

This publication is also available in English under the title *Privacy and Security Incident Management Protocol*.

Table des matières

1.0 Quel est l'objectif du *Protocole de gestion des incidents liés au respect de la vie privée et à la sécurité de l'information*?

Ce protocole permet à l'ICIS de détecter, de gérer et de résoudre les violations et les incidents liés au respect de la vie privée et à la sécurité de l'information.

Il vise tous les éléments d'actif informationnel de l'ICIS, notamment les renseignements personnels sur la santé, les renseignements personnels sur les travailleurs de la santé et les renseignements personnels sur les employés, ainsi que les systèmes d'information. Tous les employés de l'ICIS sont tenus de suivre ce protocole, y compris les employés à temps plein et à temps partiel, les employés contractuels, les sous-traitants (notamment les experts-conseils externes), les personnes en détachement, les travailleurs temporaires et les étudiants.

2.0 Qu'est-ce qu'un incident?

2.1 Constitue un incident tout événement qui

- a des répercussions ou pourrait avoir des répercussions sur la confidentialité, l'intégrité et la disponibilité de l'actif informationnel de l'ICIS;
- compromet ou pourrait compromettre les mesures de contrôle de la sécurité de l'information de l'ICIS;
- peut entraîner l'utilisation, la reproduction, la modification, la divulgation ou la destruction non autorisée des éléments d'actif informationnel de l'ICIS, ou l'accès non autorisé à ceux-ci; ou
- est une violation présumée de la vie privée ou de la sécurité de l'information.

Vous êtes tenus de signaler tous les événements qui correspondent à cette définition. Ces événements ne deviendront pas tous des incidents, mais une série d'événements pourrait en devenir un. Par exemple, une tentative d'hameçonnage infructueuse isolée ne constitue pas nécessairement un incident; toutefois, une attaque par hameçonnage ciblée et à grande échelle le serait.

2.2 Parmi les exemples d'incidents, citons

- le non-respect de la Politique de respect de la vie privée, 2010 publiée par l'ICIS et des procédures visant la diffusion des renseignements personnels sur la santé;
- le non-respect d'ententes de partage de données, d'ententes de recherche, d'ententes de confidentialité ou d'ententes avec des tiers fournisseurs de services;
- la compromission de renseignements tels que les mots de passe, les versions de logiciels, les adresses IP et l'information sur l'infrastructure de sécurité;
- la perte d'actifs de l'ICIS tels qu'ordinateurs portables, téléphones, cartes d'accès ou supports d'information amovibles (p. ex. CD, DVD, clés USB);
- les bogues d'une application informatique qui compromettent la confidentialité, l'intégrité ou la disponibilité de l'information;
- les cyberattaques ou autres activités hostiles;
- les vulnérabilités connues des applications, de l'infrastructure ou des processus qui pourraient raisonnablement mener à une compromission de la sécurité de l'information;
- la compromission de la sécurité physique, notamment du contrôle de l'accès à un périmètre;
- la corruption de données en raison d'une logique de traitement incorrecte ou d'erreurs de programmation.

3.0 Qu'est-ce qu'une violation?

3.1 Constitue une violation tout événement qui

- entraîne l'accès aux actifs informationnels de l'ICIS contenant des renseignements personnels sur la santé, des renseignements personnels sur les travailleurs de la santé, des renseignements personnels généraux ou des renseignements personnels sur les employés, ou encore l'utilisation, la reproduction, la modification, la divulgation ou la destruction de ces actifs, sans autorisation ou illégalement (c.-à-d. en violation des lois applicables comme la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario et ses règlements), de façon délibérée ou non (**violation de la vie privée**); ou
- compromet les mesures de contrôle de la sécurité de l'information de l'ICIS et, conséquemment, la confidentialité, l'intégrité ou la disponibilité d'actifs informationnels de l'ICIS (**violation de la sécurité**).

Il est important de noter qu'un incident peut constituer ou non une violation. Par exemple, l'acheminement par courriel de renseignements personnels sur la santé ou de données dépersonnalisées à un fournisseur de données **sans** d'abord avoir compressé, chiffré et protégé par un mot de passe le fichier constitue une violation du document de l'ICIS intitulé *Secure Information Transfer Standard* (en anglais seulement). Ce type d'événement est toujours classifié à titre d'incident, même si l'information est communiquée en toute sécurité au bon destinataire.

3.2 Parmi les exemples de violations, citons

- la perte ou le vol d'une clé USB contenant des renseignements personnels sur la santé non chiffrés;
- l'envoi de renseignements personnels sur la santé au mauvais destinataire ou l'accès d'une personne ou d'un organisme à des renseignements qui ne lui étaient pas destinés;
- la consultation inappropriée, c'est-à-dire à des fins non liées au travail, par les employés de fichiers de données contenant des renseignements personnels sur la santé;
- les activités malveillantes de pirates informatiques entraînant la compromission des systèmes ou du réseau de l'ICIS.

4.0 Quelle responsabilité vous incombe en vertu de ce protocole?

4.1 Vous devez **immédiatement** signaler tout incident ou toute violation à incident@icis.ca, en envoyant une copie de votre courriel à votre superviseur ou à votre gestionnaire. Vous n'avez pas à obtenir son autorisation préalable. Le courriel acheminé à incident@icis.ca avise les équipes chargées du respect de la vie privée et de la sécurité de l'information de l'incident, afin qu'elles puissent commencer à en assurer la gestion.

4.2 Dans votre courriel, vous devez décrire l'incident et indiquer notamment

- le moment où il a été découvert;
- la manière dont il a été découvert;
- l'emplacement;
- la cause (si vous la connaissez);
- les personnes visées;
- tout autre renseignement pertinent, notamment toute mesure prise sur-le-champ en vue d'en confiner les effets.

4.3 Vous devez **immédiatement** appliquer des mesures de confinement pouvant comprendre l'interruption ou l'isolement de systèmes ou de services, et pouvant être requises en même temps que le signalement ou tout de suite après. Il y a lieu de préserver les éléments de preuve lorsque des mesures de confinement sont prises (p. ex. dans le cas des incidents pouvant résulter d'actes malveillants).

5.0 Vous avez signalé l'incident — que se passe-t-il ensuite?

5.1 L'équipe d'intervention en cas d'incident (EII) sera réunie, amorcera la gestion de l'incident et communiquera avec vous si elle requiert votre participation.

> L'EII comptera sur votre collaboration immédiate et demandera que vous accordiez une grande priorité aux activités de gestion de l'incident.

5.2 L'EII déterminera les activités devant être exécutées sur-le-champ, y compris toute communication à l'interne ou à l'externe.

> Ne divulguez jamais les détails d'un incident à l'externe, puisque ce genre de renseignement pourrait présenter un risque sur le plan de la sécurité ou entacher la réputation de l'ICIS.

6.0 Activités de gestion de l'incident

Vous trouverez à l'annexe A le glossaire des termes utilisés dans le présent document et leurs définitions.

Vous trouverez à l'annexe B la liste de vérification pour la gestion des incidents.

6.1 Confinement et évaluation

6.1.1 Dès qu'un incident est signalé, l'EII de base est réunie. Elle comprend les 2 personnes suivantes :

- le chef de la sécurité de l'information (ou son délégué), soit l'autorité responsable de la gestion au quotidien du programme de sécurité de l'information de l'ICIS;
- le chef de la protection des renseignements personnels et avocat général (ou son délégué), soit l'autorité responsable de la gestion au quotidien du programme de respect de la vie privée de l'ICIS.

6.1.2 L'EII de base évalue la nature de l'incident et détermine s'il s'agit d'un incident mineur ou d'un incident majeur, ce dernier pouvant être une violation de la vie privée ou de la sécurité de l'information (voir l'annexe C : Classification des incidents — incident majeur ou mineur).

Les incidents mineurs peuvent être résolus par l'EII de base. Celle-ci peut demander ou non le concours d'autres membres. Il n'est pas obligatoire d'exécuter les autres activités de gestion des incidents énumérées dans le présent protocole s'il s'agit d'un incident mineur.

Les incidents majeurs exigent une intervention officielle en matière de gestion des incidents, laquelle intègre toutes les activités de gestion des incidents établies dans le présent protocole.

6.1.3 Les incidents majeurs nécessitent l'élargissement de l'EII. L'ajout de personnes à l'EII au-delà de l'EII de base varie selon la nature de chaque incident. Toutefois, l'EII doit comprendre au moins les membres du personnel suivants (ou leurs délégués) :

- un représentant de la direction ou de la haute direction de toutes les sections touchées au sein de l'ICIS, même s'il n'est pas tenu de participer directement aux activités de gestion de l'incident;
- un représentant de la direction ou de la haute direction de tous les services ou de toutes les divisions de technologie de l'information touchés au sein de l'ICIS;
- un représentant du Centre de services (dans le cas d'un incident visant les applications ou les technologies de l'ICIS).

6.1 4 L'EII de base informera le dirigeant principal de l'information et le vice-président, Services administratifs, de tout incident majeur.

6.1.5 L'EII de base enverra à tous les participants un courriel qui contiendra

- une description de l'incident;
- un numéro de téléphone qui permettra de joindre une téléconférence immédiate et d'effectuer tout autre appel dans le cadre des activités de gestion de l'incident;
- une liste des membres de l'EII.

6.1.6 Au cours de la première téléconférence, l'EII évaluera l'étendue de l'incident et déterminera

- le responsable de la gestion de l'incident;
- si d'autres membres du personnel doivent joindre l'EII;
- les mesures de confinement pouvant être requises, notamment l'interruption nécessaire de systèmes ou de services;
- les exigences en matière de communication, tant à l'interne qu'à l'externe;
- les préjudices éventuels ou réels en lien avec l'incident;
- toute autre exigence que dicte la nature de l'incident;
- un calendrier des prochains appels et des prochaines réunions, au besoin.

6.1.7 Si, à tout moment pendant l'enquête, l'EII détermine qu'il y a eu violation de la vie privée ou de la sécurité, il y aura lieu non seulement de confiner l'incident, mais aussi de préserver la preuve. L'EII de base informera le dirigeant principal de l'information et le vice-président, Services administratifs, de toute violation de la vie privée ou de la sécurité.

6.1.8 S'il y a violation grave de la vie privée ou de la sécurité, l'EII collaborera avec un représentant de la direction ou de la haute direction des Communications afin de coordonner la communication entre l'organisme et les intervenants externes selon les besoins.

Le responsable de la gestion de l'incident, lequel représente l'EII, a force d'autorité ultime pour parler en son nom au cours de l'enquête et des activités de confinement. Le responsable de la gestion de l'incident peut diriger le personnel dans l'exécution des activités de confinement et détient le pouvoir exclusif d'autoriser la reprise des activités ou des services ayant fait l'objet d'une interruption.

6.1.9 L'EII effectuera une évaluation préliminaire de l'incident et s'assurera que toutes les mesures de confinement appropriées ont été prises. Les mesures de confinement visent à minimiser les préjudices réels ou éventuels causés par l'incident.

L'évaluation préliminaire a pour but de déterminer l'étendue immédiate de l'incident : les données, les systèmes, les utilisateurs et les intervenants touchés.

Si l'on soupçonne que l'incident résulte d'un acte hostile, illégal, criminel ou illicite, la décision de communiquer avec les autorités et la responsabilité afférente incombent au chef de la protection des renseignements personnels et avocat général.

6.1.10 Si l'on soupçonne que l'incident pourrait entraîner une perturbation importante nécessitant la mise en œuvre du plan de continuité des opérations, l'EII de base en informera le vice-président, Services administratifs, qui agit également à titre de président de l'équipe responsable de la continuité des opérations.

6.1.11 Les mesures de confinement qui sont raisonnables dans les circonstances doivent être appliquées afin qu'aucune autre violation de la vie privée ou de la sécurité de l'information par les mêmes moyens ne puisse avoir lieu, doivent empêcher tout accès non autorisé à quelque autre renseignement et doivent prévenir n'importe quelle autre violation de la vie privée ou de la sécurité de l'information. Ces mesures peuvent comprendre les activités suivantes :

- récupérer ou détruire, de façon sécuritaire, les données ou les copies de données touchées, y compris satisfaire à l'exigence relative à l'obtention d'une confirmation écrite de la date, de l'heure et de la méthode de destruction sécuritaire;
- interrompre ou isoler les applications ou les services;
- supprimer l'accès de certaines personnes ou de certains groupes de personnes aux applications ou aux services;
- mettre en œuvre une solution de contournement temporaire ou permanente afin de confiner l'incident ou d'éviter qu'il ne se reproduise;
- apporter des changements temporaires ou permanents aux processus;
- interrompre temporairement la diffusion des applications ou les activités de production.

6.1.12 L'EII déterminera, au cas par cas, quels documents doivent être remplis et lui être fournis, y compris le calendrier.

Si les mesures de confinement risquent de perturber considérablement la continuité des activités, l'EII doit envisager la possibilité de faire état de la situation au président-directeur général, à la Direction des communications ou à d'autres personnes, ou de demander leur aide, au besoin.

L'EII doit aviser le plus rapidement possible le président-directeur général de toute violation présumée ou réelle de la vie privée ou de la sécurité de l'information. L'EII déterminera, au cas par cas, la forme de cet avis (p. ex. verbale ou écrite) et le type de renseignement qui devra alors être fourni au président-directeur général.

6.1.13 Un membre de l'EII peut demander verbalement à un employé d'instaurer une mesure de confinement sans d'abord effectuer les processus de gestion du changement en vigueur. Toutefois, dans une telle situation, les exigences liées au processus de gestion du changement doivent être satisfaites par la suite le plus rapidement possible.

6.1.14 L'EII doit

- déterminer le processus à suivre pour l'examen des mesures de confinement mises en œuvre, et déterminer si la violation de la vie privée ou de la sécurité de l'information a bien été confinée ou si d'autres mesures de confinement sont nécessaires;
- déterminer, au cas par cas, quels documents doivent être fournis à l'EII aux fins de l'examen des mesures de confinement et ce qu'ils doivent contenir.

Il y a lieu de préserver les éléments de preuve dans le cadre de l'enquête et des activités de confinement d'un incident. En particulier, si l'incident peut résulter d'actes malveillants, ou si on peut raisonnablement s'attendre à ce qu'un incident donne lieu à une poursuite en justice, l'ICIS fera appel à une firme indépendante d'experts judiciaires. Dans tous les cas, les membres du personnel devront tout mettre en œuvre pour que soient conservés les éléments de preuve tels que les fichiers de journalisation, les fichiers de cache, la copie des flux binaires et les communications. Toutefois, si ces mesures de conservation font en sorte d'accroître les préjudices liés ou pouvant être liés à l'incident, en augmentant par exemple l'étendue ou la probabilité d'une violation de la vie privée ou de la sécurité de l'information, mieux vaut alors accorder la priorité au confinement de l'incident. Le chef de la protection des renseignements personnels et le chef de la sécurité de l'information en décideront.

6.2 Communication et processus d'avis

6.2.1 La communication constitue un élément essentiel de la gestion des incidents. La communication interne permet aux membres du personnel de comprendre la situation ainsi que les répercussions et activités d'atténuation qui lui sont associées. La communication externe renseigne les intervenants sur l'étendue et la durée prévue de l'incident.

6.2.2 L'EII, en collaboration avec d'autres participants au besoin, dirigera les communications internes et externes requises. Vous **ne devez** communiquer **aucun** renseignement concernant un incident à l'externe, à moins d'en avoir d'abord reçu la directive de l'EII.

S'il y a violation de la vie privée ou de la sécurité de l'information, le processus d'avis (c.-à-d. à quel moment envoyer l'avis, comment le faire, qui devrait le faire et quels éléments y inclure) sera déterminé par le président-directeur général, en consultation avec l'EII. Ce processus sera établi au cas par cas, en tenant compte des lignes directrices et des autres documents publiés par les commissaires à la protection de la vie privée ou les autres autorités de réglementation, et conformément à toute exigence spécifique énoncée dans les lois et règlements et dans les ententes avec les fournisseurs de données.

6.2.3 Si le président-directeur général détermine que les renseignements personnels sur la santé visés proviennent de l'Ontario, l'ICIS doit

- aviser à la première possibilité raisonnable le dépositaire des renseignements sur la santé ou l'autre organisme ayant divulgué à l'ICIS les renseignements personnels sur la santé si des renseignements personnels sur la santé ont été ou peuvent avoir été volés, perdus ou consultés par des personnes non autorisées ou dans un autre cas prévu dans l'entente avec ce dépositaire ou cet organisme;
- aviser le dépositaire des renseignements sur la santé ou l'autre organisme de l'étendue de la violation de la vie privée ou de la sécurité de l'information, du type de renseignements personnels sur la santé visés, des mesures mises en œuvre pour confiner la violation de la vie privée ou de la sécurité de l'information et des autres mesures, par exemple d'enquête et de correction, qui seront prises au regard de la violation;
- aviser le dépositaire des renseignements sur la santé ou l'autre organisme en respectant la forme prévue de l'avis et en incluant l'information devant être fournie, comme déterminé par le président-directeur général en consultation avec l'EII.

6.2.4 Toute violation de la vie privée ou de la sécurité de l'information sera signalée au Conseil d'administration de l'ICIS (voir l'annexe D : Classification des violations de la vie privée ou de la sécurité de l'information). Le Conseil d'administration de l'ICIS doit aussi être avisé des résultats de toute recommandation consécutive à une enquête sur une violation de la vie privée ou de la sécurité de l'information et des progrès de leur mise en œuvre.

6.3 Enquête, correction et prévention des incidents futurs

6.3.1 Il est important de bien comprendre les événements qui ont mené à un incident afin

- d'éviter d'autres incidents semblables;
- de continuellement améliorer notre position au chapitre du respect de la vie privée et de la sécurité en tirant des leçons des incidents.

6.3.2 Il incombe à l'EII de déterminer, dans la mesure du possible, la cause principale de l'incident, ainsi que les mesures correctives qui permettront de minimiser le risque de récurrence. Ces mesures correctives peuvent être formulées dans le cadre de recommandations officielles intégrées à un rapport d'incident.

6.3.3 L'EII doit produire un rapport d'incident à l'égard de tous les incidents majeurs ou lorsqu'elle le juge nécessaire. Le rapport d'incident doit être rédigé en temps opportun, habituellement dans les 3 mois suivant l'incident.

6.3.4 L'EII soumettra pour examen le rapport d'incident qui contient ses recommandations au Comité sur le respect de la vie privée, la confidentialité et la sécurité. Le rapport sera ensuite transmis au Comité de la haute direction afin que toute recommandation puisse être ajoutée au registre principal des plans d'action. Les recommandations préciseront qui sera chargé de mettre en œuvre les recommandations, d'établir l'échéancier de mise en œuvre de ces recommandations, et de veiller à ce que la mise en œuvre se fasse dans les délais fixés.

6.3.5 Le chef de la sécurité de l'information ou le chef de la protection des renseignements personnels peut, à sa discrétion, demander que la mise en œuvre de certaines recommandations soit terminée avant la clôture de l'incident. Le chef de la sécurité de l'information ou le chef de la protection des renseignements personnels déterminera les possibilités de formation ou de sensibilisation dans le cadre du processus de gestion des incidents et agira en conséquence.

6.4 Registre des violations de la vie privée

6.4.1 Le Secrétariat à la vie privée et aux services juridiques a créé un registre des violations de la vie privée qui comporte les éléments suivants :

- la date de la violation de la vie privée;
- la date à laquelle la violation de la vie privée a été constatée ou soupçonnée;
- l'origine (interne ou externe) de la violation de la vie privée;
- le type de renseignement personnel sur la santé ayant fait l'objet de la violation de la vie privée de même que la nature et l'étendue de la violation de la vie privée;
- la date à laquelle la violation de la vie privée a été confinée et la description des mesures de confinement mises en œuvre;
- s'il y a lieu, la date à laquelle le dépositaire des renseignements sur la santé ou l'organisme ayant divulgué à l'ICIS les renseignements personnels sur la santé a été avisé;
- la date à laquelle l'enquête sur la violation de la vie privée a pris fin;
- le nom de la ou des personnes chargées de mener l'enquête.

6.4.2 Le Secrétariat à la vie privée et aux services juridiques tient également un registre de toutes les recommandations liées au respect de la vie privée qui comporte les éléments suivants :

- les recommandations découlant de l'enquête;
- le nom du gestionnaire chargé de mettre en œuvre chaque recommandation;
- la date à laquelle chaque recommandation a été ou doit être mise en œuvre;
- la mesure qui a été ou doit être prise pour mettre en œuvre chaque recommandation.

6.5 Registre des violations de la sécurité de l'information

6.5.1 Le secteur Sécurité de l'information a créé un registre des violations de la sécurité de l'information qui comporte les éléments suivants :

- la date de la violation de la sécurité de l'information;
- la date à laquelle la violation de la sécurité de l'information a été constatée ou soupçonnée;
- le type de renseignement personnel sur la santé, le cas échéant, ayant fait l'objet de la violation de la sécurité de l'information de même que la nature et l'étendue de la violation de la sécurité de l'information;
- la date à laquelle la violation de la sécurité de l'information a été confinée et la description des mesures de confinement mises en œuvre;

- la date à laquelle le dépositaire des renseignements sur la santé ou l'organisme ayant divulgué à l'ICIS les renseignements personnels sur la santé a été avisé, le cas échéant;
- la date à laquelle l'enquête sur la violation de la sécurité de l'information a été terminée;
- le nom de l'agent ou des agents (employés) chargés de mener l'enquête.

6.5.2 Le secteur Sécurité de l'information tient également un registre de toutes les recommandations liées au respect de la sécurité de l'information qui comporte les éléments suivants :

- les recommandations découlant de l'enquête;
- le nom de l'agent ou des agents (employés) chargés de mettre en œuvre chaque recommandation;
- la date à laquelle chaque recommandation a été ou doit être mise en œuvre;
- la mesure qui a été ou doit être prise pour mettre en œuvre chaque recommandation.

6.6 Respect, vérification et application

Le Code de conduite de l'ICIS (en anglais seulement) définit les comportements éthiques et professionnels au chapitre des relations, des renseignements, y compris des renseignements personnels sur la santé, et du milieu de travail. Tout le personnel est tenu de se conformer au code ainsi qu'aux politiques, procédures et protocoles de l'ICIS. La conformité aux politiques, procédures et protocoles en matière de respect de la vie privée et de sécurité est encadrée par les programmes de vérification du respect de la vie privée et de la sécurité de l'ICIS. Les contraventions au code sont référées aux Ressources humaines, au besoin, et peuvent entraîner des mesures disciplinaires allant jusqu'au congédiement.

Avis de violation

Les cas de non-conformité aux politiques en matière de respect de la vie privée et de sécurité sont traités conformément à ce protocole, en vertu duquel le personnel doit signaler tout incident ou toute violation à incident@icis.ca.

Annexes

Annexe A : Glossaire

actif informationnel

Fait partie de l'actif informationnel tout fichier électronique ou document papier qui contient de l'information, notamment les bases de données et les ensembles de données.

confidentialité

Seules les personnes détenant l'autorisation voulue peuvent consulter, utiliser, reproduire ou divulguer l'information. La confidentialité est essentielle, mais ne suffit pas à assurer le respect de la vie privée.

disponibilité

Par disponibilité s'entend le bon fonctionnement de l'information, des systèmes d'information et des diverses mesures de contrôle de la sécurité, d'une manière qui permet aux utilisateurs autorisés d'avoir accès aux données au moment et de la façon souhaités.

équipe d'intervention en cas d'incident

Équipe spéciale qui, à titre de comité directeur, examine tous les aspects du confinement de l'incident, des mesures d'intervention et de la production d'un rapport d'incident.

équipe d'intervention en cas d'incident de base

- Chef de la sécurité de l'information (ou son délégué)
- Chef de la protection des renseignements personnels et avocat général (ou son délégué)

intégrité

Par intégrité s'entend le fait qu'aucune donnée ne peut être créée, modifiée, ni supprimée sans autorisation, ce qui permet d'avoir confiance en leur vraisemblance.

mesure de contrôle de la sécurité de l'information

Mesure visant à atténuer les risques liés à la sécurité de l'information. Les mesures de contrôle peuvent être de nature administrative (p. ex. des processus et des procédures), logique (p. ex. des mesures de contrôle techniques comme des coupe-feu et des mots de passe) ou physique (p. ex. des mesures de contrôle visant l'environnement physique comme le contrôle de l'accès à un périmètre et les dispositifs de prévention des incendies).

renseignements personnels généraux

Renseignements personnels sur une personne identifiable, notamment les renseignements sur l'origine raciale ou ethnique et la nationalité, la couleur de la peau, la religion, l'âge, le sexe, l'orientation sexuelle ou l'état matrimonial de la personne; le niveau de scolarité ou les antécédents médicaux, criminels et professionnels de la personne; tout numéro d'identification, symbole ou autre élément particulier attribué à la personne; l'adresse, les empreintes digitales ou le groupe sanguin de la personne.

renseignements personnels sur la santé (RPS)

Renseignements sur la santé d'une personne qui

- permettent d'identifier cette personne; ou
- peuvent être utilisés ou manipulés selon une méthode raisonnablement prévisible pour identifier cette personne, ou qui peuvent être associés, au moyen d'une méthode raisonnablement prévisible, à d'autres renseignements qui identifient la personne.

renseignements personnels sur les employés

Renseignements personnels sur une personne qui sont recueillis, utilisés ou communiqués aux fins d'établissement, de gestion ou de cessation d'une relation d'emploi entre l'ICIS et cette personne. Ils comprennent notamment des renseignements ayant trait au processus d'embauche, à l'administration de la rémunération et des programmes d'avantages sociaux, aux évaluations du rendement, aux mesures disciplinaires et à la planification de l'avancement.

renseignements personnels sur les travailleurs de la santé

Renseignements au sujet d'un dispensateur de services de santé qui identifient ou pourraient identifier une personne selon une méthode raisonnablement prévisible, tel que défini dans la *Politique de respect de la vie privée relative à la collecte, à l'utilisation, à la divulgation et à la conservation des renseignements personnels des travailleurs de la santé et des données dépersonnalisées, 2011* de l'ICIS.

responsable de la gestion de l'incident

Personne à qui il incombe de gérer tous les aspects du confinement de l'incident, des mesures d'intervention et de la production du rapport d'incident, et notamment de convoquer l'équipe d'intervention en cas d'incident.

Annexe B : Liste de vérification pour la gestion des incidents

Responsable	Activité	Mesure prise
EII de base	Envoyer un premier courriel contenant les éléments suivants : • l'horaire de la première téléconférence, y compris le numéro de téléphone de liaison et le code d'accès qui serviront dans le cadre de toutes les réunions • les renseignements concernant l'incident • la composition de l'EII	s.o.
EII de base	Identifier les membres qui formeront l'EII	s.o.
EII de base	Classifier l'incident	Incident majeur ou mineur
EII de base	Consigner la demande de gestion de l'incident au Centre de services	s.o.
EII	Nommer un responsable de la gestion de l'incident	s.o.
EII	Établir les mesures de confinement	s.o.
EII, communication	Définir les exigences en matière de communication interne; établir un plan de communication en cas de crise, selon les besoins	s.o.
EII, communication	Définir les exigences en matière de communication externe; établir un plan de communication en cas de crise, selon les besoins	s.o.
EII	Planifier les appels de suivi, au besoin	s.o.
CPRP/AG	Communiquer avec les autorités au sujet de toute activité illégale, criminelle ou illicite	s.o.
EII	Aviser le PDG de la situation (obligatoire en cas de violation présumée de la vie privée ou de la sécurité de l'information ou selon la décision de l'EII)	s.o.
EII	Rédiger un rapport d'incident ou de violation	s.o.

Remarques
EII : équipe d'intervention en cas d'incident.
CPRP/AG : chef de la protection des renseignements personnels et avocat général.
s.o. : sans objet.

Annexe C : Classification des incidents — incident majeur ou mineur

La classification d'un incident est une activité subjective. L'EII doit tenir compte de différents facteurs, notamment

- des préjudices réels ou éventuels;
- de l'étendue et de la durée de l'incident;
- de la nature des mesures de confinement requises, le cas échéant;
- de la cause principale;
- de la nature délicate ou non de l'information touchée.

Exemples de classification d'un incident

Incident	Classification	Justification
Cas isolé de divulgation inappropriée de renseignements dépersonnalisés en raison d'une erreur humaine	Mineur	• Il ne s'agit pas de renseignements personnels sur la santé. • L'incident n'a causé aucun préjudice à des personnes ou à des clients de l'ICIS. • Il ne s'agit pas d'une situation récurrente. • Il ne s'agit pas d'une erreur d'application.
Attaque d'un logiciel malveillant contre un seul ordinateur et ayant été confinée avec succès	Mineur	• Le problème n'est pas généralisé. • L'incident n'a causé aucun préjudice aux systèmes ou à l'information de l'ICIS.
Diffusion de renseignements selon une méthode autre que celles approuvées	Mineur	• Les renseignements ont été transmis à la bonne personne. • L'incident n'a causé aucun préjudice à des personnes ou à des clients de l'ICIS. • Il ne s'agit pas d'une situation récurrente. • Il ne s'agit pas d'une erreur d'application.
Toute violation de la vie privée ou de la sécurité	Majeur	• Par définition, toutes les violations de la vie privée ou de la sécurité constituent des incidents majeurs.
Une erreur d'application entraîne la divulgation de rapports électroniques au mauvais établissement	Majeur	• L'incident pourrait causer des préjudices éventuels à des personnes ou à des clients de l'ICIS. • Le problème pourrait être généralisé. • Il convient généralement d'interrompre les systèmes à des fins de confinement.

Annexe D : Classification des violations de la vie privée ou de la sécurité de l'information

Outil d'évaluation du risque en cas de violation de la vie privée ou de la sécurité de l'information

Objectif : Permettre à l'ICIS d'évaluer l'incidence d'une violation de la vie privée ou de la sécurité de l'information et la probabilité que cette dernière entraîne des préjudices.

Étape 1

Incidence de la violation		Négligeable	Faible	Moyenne	Très grande	Extrême
A	Ampleur de la violation (nombre de personnes, nombre de provinces et de territoires, au Canada ou ailleurs)	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
B	Type et nature délicate ou non des renseignements qui ont été touchés (données cliniques)	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
C	Nombre d'éléments de données différents qui ont été touchés (total approximatif)	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
D	Autres facteurs ou points à prendre en compte					

Incidence globale de la violation Faible/moyenne/élevée	F	M	É

Étape 2

Probabilité de préjudice		Rare	Peu probable	Modérée	Probable	Presque certaine
E	Destinataire connu : public en général, personne déterminée, groupe déterminé de personnes (en vertu d'une entente de confidentialité) ou groupe déterminé de personnes (en vertu des lois et des règlements)	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
F	Cause de la violation : accidentelle (erreur humaine), systémique ou intentionnelle (intention malveillante, risque de vol d'identité)	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
G	Préjudice découlant de la violation (probabilité que l'information ait été indûment utilisée, ou le soit un jour, à des fins frauduleuses ou préjudiciables : préjudice physique, préjudice financier, atteinte à la sécurité, atteinte à la réputation ou tout autre préjudice causé à la personne)	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
H	Autres facteurs ou points à prendre en compte					

Probabilité globale de préjudice Faible/moyenne/élevée	F	M	É

aide@icis.ca

ICIS Ottawa
495, chemin Richmond
Bureau 600
Ottawa (Ont.)
K2A 4H6
613-241-7860

ICIS Toronto
4110, rue Yonge
Bureau 300
Toronto (Ont.)
M2P 2B7
416-481-2002

ICIS Victoria
880, rue Douglas
Bureau 600
Victoria (C.-B.)
V8W 2B7
250-220-4100

ICIS Montréal
1010, rue Sherbrooke Ouest
Bureau 602
Montréal (Qc)
H3A 2R7
514-842-2226

icis.ca

23460-1022