BC Society of Transition Houses

Vie privée, sécurité et confidentialité:

Considérations liées aux bases de données pour les organisations antiviolence au Canada

BC Society of Transition Houses

REMERCIEMENTS

Recherche, rédaction, révision:

Rhiannon Wong
Nicky Bowman
Tanyss Knowles
Louise Godard
Amy S. FitzGerald

Traduction française: Michele Briand

Conception graphique: *Hannah Lee*

Des sections du présent document ont été adaptées à partir du Safety Net Technology Project du National Network to End Domestic Violence, États-Unis, et en coopération avec eux.

Cette ressource actualisée a été financée par le Commissariat à la protection de la vie privée du Canada (CPVPC). Les perspectives et opinions exprimées sont celles de la BC Society of Transition Houses et ne reflètent pas nécessairement celles du CPVPC.

La première édition du présent guide a été publiée en 2012. Recherche, rédaction et révision par:

Cynthia Fraser
Rhiannon Wong
Laurie Parsons

Traduction française: *Jose Beaudet*

Conception graphique: *Hannah Lee*

BC Society of Transition Houses

TABLE DES MATIÈRES

CONTEXTE

La BC Society of Transition Houses (BCSTH) a reçu une subvention du Commissariat à la protection de la vie privée du Canada pour:

- Mener une recherche sur l'utilisation des bases de données comme technologie d'amélioration de la confidentialité (TAC) par les organisations antiviolence au Canada
- Enquêter auprès des fournisseurs quant à la sécurité de leurs bases de données et la capacité de ces dernières d'améliorer la vie privée des femmes, enfants et jeunes qui subissent la violence familiale et/ou sexuelle
- Développer des ressources pratiques pour les organisations antiviolence utilisant présentement ou prévoyant utiliser une base de données dans le cadre de leur travail.

Les organisations antiviolence offrent un continuum de services visant un objectif commun: soutenir les femmes, les enfants et les jeunes qui subissent la violence familiale et/ou sexuelle.

En 2012, financée par le Commissariat à la protection de la vie privée du Canada, la BCSTH a entrepris des recherches sur l'utilisation de la technologie et de son intersection avec la violence faite aux femmes. La première version de «Privacy, Security, and Confidentiality: Database Considerations for Violence against Women Programs» était l'une des ressources développées à partir des recherches initiales de la BCSTH. Plus que jamais, la collecte et le stockage électroniques de renseignements personnels concernant les femmes, les enfants et les jeunes qui accèdent à des organisations antiviolence demeurent un important sujet de discussion parmi ces organisations et les bailleurs de fonds.

Selon le personnel des organisations antiviolence, les bases de données servent à uniformiser la collecte et le stockage des renseignements personnels[1] et rendent les données plus accessibles. Toutefois, dans le contexte de femmes, d'enfants et de jeunes subissant de la violence familiale et sexuelle et du harcèlement, ou qui sont victimes de la traite des personnes, le stockage de leurs renseignements personnels dans une banque de données peut mettre leur sécurité à risque par le biais d'interceptions en ligne, d'assignations, de requêtes par des tierces parties et de fuites de données. Pour ces motifs, il

[1] Renseignements personnels est le terme utilisé dans la Loi sur la protection des renseignements personnels et les documents électroniques et défini comme «tout renseignement concernant un individu identifiable» (voir la *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, ch. 5), Article 2(1), Définitions). On peut trouver une définition beaucoup plus complète des renseignements personnels, y compris de nombreux exemples de ce qui peut constituer des «renseignements personnels», dans la Loi sur la protection des renseignements personnels (L.R.C., 1985, ch. P-21), Article 3, Définitions. D'autres termes sont parfois utilisés comme synonymes de renseignements personnels, notamment, données à caractère personnel (voir, par exemple, le GDPR, Article 4(1)) ou renseignements permettant d'identifier un individu (voir, par exemple, National Institute of Standards and Technology (NIST) Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), datée d'avril 2010).

est préférable pour les organisations antiviolence de ne récolter et stocker les renseignements personnels concernant les femmes, les enfants et les jeunes qui sont ***nécessaires*** à la livraison de services et seulement pour le temps requis.

La *Loi sur la protection des renseignements personnels* du Canada définit les renseignements personnels comme les «renseignements, quels que soient leur forme et leur support, concernant un individu identifiable». Il peut s'agir de «renseignements relatifs à sa race, à son origine nationale ou ethnique, à sa couleur, à sa religion, à son âge ou à sa situation de famille; à son groupe sanguin, à ses empreintes digitales; à son dossier médical, à son casier judiciaire, à ses antécédents professionnels; à des opérations financières auxquelles il a participé; à son adresse; à tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre [assurance sociale, permis de conduire, etc.][2]. Toutes les bases de données commerciales et le Système d'information sur les personnes et les familles sans abri du Canada (SISA) récoltent des renseignements personnels dans leurs bases de données standard.

En raison de la nature délicate et complexe de la collecte de renseignements personnels, la BCSTH reçoit régulièrement des demandes de la part d'organisations et de bailleurs de fonds antiviolence du Canada au sujet de leurs préoccupations concernant les bases de données électroniques et la protection de la vie privée des femmes. Dans le but de leur offrir le soutien nécessaire, la BCSTH a étudié l'utilisation par les organisations antiviolence de bases de données électroniques et les impacts sur la sécurité et la vie privée de la collecte et du stockage électronique des renseignements personnels de femmes, d'enfants et de jeunes. En 2018, la BCSTH a mené deux sondages en ligne:

- «Utilisation de bases de données et de système de gestion de cas électroniques par des organisations antiviolence de tout le Canada» a été distribué en français et en anglais à des organisations antiviolence de tout le Canada.
- «Database Questionnaire for the BC Society of Transition Houses». Ce sondage a été distribué à des fournisseurs de bases de données électroniques et des administrateurs du SISA identifiés par du personnel antiviolence et des experts en sécurité comme étant accessibles au Canada.

Le présent rapport examinant les bases de données est l'une de trois ressources issues des résultats d'un sondage mené en 2018, de conversations avec des spécialistes antiviolence en matière de confidentialité, de démonstrations de fournisseurs de bases de données, d'échanges avec des bailleurs de fonds et de consultations auprès d'associations provinciales offrant du soutien aux maisons d'hébergement pour femmes violentées. Ce rapport vise à accompagner et guider les organisations antiviolence dans le processus complexe de réflexion entourant la mise en œuvre d'une base de données électronique visant à récolter et stocker les renseignements personnels de femmes, d'enfants et de jeunes subissant la violence familiale et la violence sexuelle. Les organisations antiviolence, qui

[2] Commissariat à la protection de la vie privée du Canada. (2016). Le gouvernement fédéral et vos renseignements personnels. Tiré de: https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/votre-droit-a-la-vie-privee/le-gouvernement-federal-et-vos-renseignements-personnels/

envisagent l'acquisition d'une base de données ou qui en utilisent une présentement, sont encouragées à lire ce rapport pour évaluer les risques et les avantages des différentes bases de données. Ce rapport veut aider les organisations antiviolence à prendre des décisions informées en vue de s'assurer que soient protégées la sécurité, la vie privée et la confidentialité des femmes, des enfants et des jeunes. L'interception, l'atteinte et/ou l'accès non autorisé aux renseignements personnels des récipiendaires de services qui accèdent aux organisations antiviolence peut mettre en péril la sécurité et la vie de femmes, d'enfants et de jeunes.

Les lois suivantes sur la protection de la vie privée sont mentionnées dans le présent rapport:

- Personal Information and Protection Act (PIPA) pour les organisations basées en Colombie-Britannique;
- Personal Information and Protection Act (PIPA) pour les organisations basées en Alberta;
- *Loi sur la protection des renseignements personnels* pour les pratiques d'utilisation des renseignements personnels par les ministères et organismes gouvernementaux;
- *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) pour l'utilisation des renseignements personnels par les entreprises commerciales canadiennes.

Les organisations antiviolence doivent déterminer quelles sont les lois sur la protection de la vie privée qui s'appliquent à leur organisation et leur juridiction.

Enfin, le présent rapport devrait être utilisé en conjonction avec d'autres ressources, incluant:

- Les lois provinciales et territoriales sur la protection de la vie privée
- La *Freedom of Information and Protection of Privacy Act* en Colombie-Britannique: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00
  Et la *Loi sur l'accès à l'information et la protection de la vie privée* en Ontario: https://www.ontario.ca/fr/lois/loi/90f31
- Les lois provinciales et territoriales sur la protection de l'enfance et de la jeunesse
- Le Code criminel du Canada https://laws-lois.justice.gc.ca/fra/lois/c-46/
- La *Loi sur la protection des renseignements personnels* https://www.canlii.org/fr/ca/legis/lois/lrc-1985-c-p-21/derniere/lrc-1985-c-p-21.html
- La *Loi sur la protection des renseignements personnels et les documents électroniques* https://www.canlii.org/fr/ca/legis/lois/lc-2000-c-5/derniere/lc-2000-c-5.html
- Trousse à outils sur la protection de la vie privée www.bchousing.org/Partners/H_S_Op/Privacy_tools
- Trousse à outils sur la gestion des dossiers des organisations à but non lucratif www.bchousing.org/Partners/H_S_Op/Administration/Records_management

- BCSTH «Legal Toolkit: General Information about Legal Issues and Court Matters in British Columbia» https://bcsth.ca/publications/bcsth-legal-toolkit-general-information-about-legal-issues-and-court-matters-in-british-columbia/
- BCSTH «Use of Technology Policy Template Guide for BC's Prevention, Education, Advocacy, Counselling and Empowerment (PEACE) organizations for children and youth experiencing violence»

QU'EST-CE QU'UNE BASE DE DONNÉES?

Les bases de données sont des programmes informatiques servant à organiser l'information de manière facile à localiser, accessible et actualisée. Les bases de données peuvent être organisée de multiples façons (notamment par ordre alphabétique ou numérique) et peuvent inclure du texte, des mots et des images. On peut effectuer des recherches dans les bases de données au moyen d'une «requête» (nom, lieu ou date) pour trouver des renseignements concernant des individus ou des groupes de personnes. La plupart des bases de données ont une fonction «rapport» qui permet de produire des rapports. Par exemple, un rapport sur le nombre de nouveaux résidents ou participants à une organisation au cours du dernier mois, ou un rapport sur la ressource la plus fréquentée.

Les bases de données permettent habituellement de créer des codes d'identification et des mots de passe, et d'établir des niveaux d'accès et des permissions d'utilisation pour le personnel ou les bénévoles identifiés comme ayant besoin d'accéder à la base de données pour leur travail. Il est de bonne pratique qu'une personne dans l'organisation soit responsable de la base de données, comme la directrice ou le directeur, quelqu'un du personnel de gestion des programmes ou de celui des technologies de l'information (TI).

De plus, les bases de données bien conçues intègrent une fonction de vérification qui peut fournir un compte rendu détaillé des demandes et actions de chaque utilisatrice ou utilisateur. Les bases de données peuvent être conçues dès le départ pour personnaliser les champs de données, produire des rapports, supprimer automatiquement des données spécifiques après une certaine période, ou retenir seulement les éléments nécessaires à la production de rapports.

TYPES DE BASES DE DONNÉES

Il existe deux options de bases de données accessibles aux organisations antiviolence du Canada. La première est une base de données personnelles, et la deuxième, une base de données de gestion des cas. Il est important pour les organisations antiviolence de tenir compte de leur capacité interne; du nombre d'organisations et de personnel qui vont utiliser la base de données; de leur budget et de leur infrastructure technologique; et des questions de sécurité, avant de prendre une décision au sujet du type de base de données à mettre en œuvre dans leur organisation.

A. Base de données personnelles

Certaines organisations antiviolence préfèrent ne récolter que les renseignements personnels de base des femmes, enfants et jeunes, tels leur nom et leurs coordonnées. Ce type de base de données est habituellement hébergée sur le serveur de l'organisation. Il existe des bases de données personnelles commerciales disponibles au Canada, mais de nombreuses organisations antiviolence canadiennes utilisent des applications logicielles comme Microsoft Acess ou Excel.

Une autre option de base de données personnelles consiste à l'utiliser comme un catalogue sur fiches faisant référence à des dossiers papier. «Dans ce cas, les données sont entrées avec un code non identifiant au lieu d'un nom. Les dossiers papier sont identifiés par le même code, ce qui aide le personnel à savoir dans quel classeur se trouve le dossier papier[3]» Cette formule est une garantie de confidentialité parce que les noms ne sont pas directement entrés dans le dossier électronique d'une femme.

Si les organisations optent pour une base de données personnelles, elles doivent évaluer les risques à la vie privée, la confidentialité et la sécurité de leur infrastructure interne de TI. Par exemple, si leur base de données est hébergée sur un ordinateur ou un serveur connecté à internet, les données personnelles stockées dans ces bases de données demeurent à risque d'être compromises par de tierces parties non autorisées. Cela peut se produire par interception des données personnelles ou par accès non autorisé si le dossier ou la base de données est entreposée dans une installation de stockage en nuage[4].

Avant de collecter et stocker des données personnelles concernant des femmes, des enfants et des jeunes dans une base de données, les organisations doivent:

- procéder à un audit de leurs TI;
- se procurer et installer toutes les applications et tous les logiciels de sécurité nécessaires;
- avoir un plan et un budget pour mettre à jour, installer et renouveler annuellement les produits de confidentialité et de sécurité en vue de s'assurer que les renseignements personnels des femmes, des enfants et des jeunes ne soient pas à risque;
- identifier les options d'entreposage, tels le stockage en nuage, et leurs risques.

B. Base de données de gestion des cas

De plus en plus, les organisations antiviolence explorent l'utilisation de base de données comme outil de gestion des cas. En plus de stocker les renseignements personnels des femmes, des enfants et des jeunes, les bases de données de gestion des cas peuvent récolter et stocker de nombreux renseignements personnels au sujet des récipiendaires de services tout en fournissant des champs

[3] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. Retrieved from: https://nnedv.org/mdocs-posts/selecting-a-database/

[4] Pour plus d'information sur les risques associés avec le stockage en nuage, voir la Section: Atteintes à la vie privée et stockage de renseignements personnels: Bases de données hébergées à distance.

pour les notes de cas, les références, la gestion des lits et la gestion des horaires du personnel. Les bases de données de gestion des cas permettent également d'exporter des rapports. Les organisations antiviolence peuvent décider de personnaliser les champs de leur base de données pour recueillir les statistiques exigées par leur bailleur de fonds et générer des rapports sommaires sur une base trimestrielle ou annuelle.

La plupart des bases de données de gestion des cas sont inscrites sur le web et exigent un appareil pouvant être connecté à internet pour y accéder. Des bases de données de gestion des cas sur serveur sont disponibles, mais l'ordinateur ou le serveur hôtes seront vraisemblablement connectés à internet. Malgré l'avantage que représente le fait d'être connecté à internet, l'accessibilité constitue également l'un des enjeux les plus sensibles. Que les renseignements personnels de femmes, d'enfants et de jeunes soient accessibles sur internet les rend vulnérables aux interceptions et accès non autorisés. Cela peut avoir des répercussions directes sur leur sécurité.

Si une organisation décide d'utiliser une base de données accessible par des appareils connectés à internet, les pratiques suivantes sont recommandées:

- élaboration de politiques qui assurent le respect des lois sur la vie privée
- consentement informé explicite des récipiendaires de services
- capacité de supprimer des renseignements de façon permanente
- pratiques très strictes de respect de la confidentialité pour réduire les risques d'atteinte à la confidentialité ou la vie privée.

Par exemple, de nombreuses organisations ayant des bases de données hébergées sur internet ont des politiques concernant quels appareils peuvent utiliser les membres du personnel pour y accéder. Dans plusieurs cas, les bases de données hébergées sur internet sont inaccessibles aux téléphones intelligents et aux ordinateurs n'appartenant pas à l'organisation.

Avant de procéder à la mise en œuvre d'une base de données, nous suggérons aux organisations d'avoir en place des infrastructures technologiques et des clés de cryptage actualisées, des politiques précises concernant l'utilisation des bases de données et des mécanismes d'administration et de surveillance.

QUELS SONT LES PROBLÈMES RÉSOLUS PAR UNE BASE DE DONNÉES?

Avant de se procurer une base de données pour le stockage des renseignements personnels de femmes, d'enfants et de jeunes, il est utile pour les organisations antiviolence *d'identifier clairement le problème* qu'elles tentent de résoudre. Pour de nombreuses organisations, l'attrait d'une base de données réside dans la facilité apparente avec laquelle elle pourra assurer le suivi des résultats, les mesurer, les utiliser pour démontrer l'efficacité de l'organisation et identifier des domaines susceptibles d'être améliorés.

Pour d'autres, c'est un moyen de collecter des données statistiques sur les activités du personnel à des fins de reddition de comptes.

Il existe sur le marché de nombreux produits dans le secteur des bases de données pour les organisations antiviolence. L'identification de leurs problèmes ou de leurs objectifs les aidera grandement à choisir le produit le mieux adapté à leurs besoins et leur épargnera peut-être aussi du temps et de l'argent. Par exemple:

- Est-ce que l'équipe éprouve des difficultés à localiser l'information dont vous avez besoin?
    - Existe-t-il une autre façon de la trouver?
    - Cette information sera-t-elle toujours utile à localiser, ou s'agit-il d'un besoin temporaire?
- Recherchez-vous un moyen plus facile de produire des rapports pour les bailleurs de fonds?
    - Les bailleurs de fonds peuvent-ils installer un système plus convivial?
- Votre organisation est-elle en processus d'obtention d'un agrément?
    - La base de données est-elle une exigence du processus d'obtention d'un agrément ou simplement une suggestion?
- Votre organisation est-elle à la recherche d'un moyen respectueux de l'environnement de conserver des dossiers?
    - Quelle est la façon la plus sécuritaire de conserver des dossiers?
- Est-ce qu'une base de données va vous fournir la meilleure option pour améliorer la sécurité, la vie privée, la confidentialité et la capacité de vivre une vie libre de violence des femmes?

ÉVALUATION DES BESOINS

Veuillez répondre aux questions suivantes avant de décider si votre organisation a besoin ou non d'une base de données:

- Comment une base de données va-t-elle vous aider à remplir la mission de votre organisation?
- L'utilisation d'une base de données est-elle conforme aux valeurs de votre organisation?
- L'utilisation d'une base de données peut-elle résulter en un surplus de temps passé par le personnel et les bénévoles devant l'ordinateur et moins avec les femmes, les enfants et les jeunes?
- L'utilisation d'une base de données va-t-elle exiger du personnel qu'il pose aux femmes, enfants et jeunes des questions pouvant influencer la nature de leurs relations, de manière négative ou positive?
- Êtes-vous en mesure d'assurer la sécurité et la confidentialité des données récoltées?

- Avez-vous la capacité d'élaborer des politiques en matière d'utilisation de la base de données et de former le personnel à cette utilisation?
- Avez-vous le soutien nécessaire en matière de TI pour héberger une base de données en toute sécurité?
- Le partage d'information concernant les femmes, les enfants et les jeunes par le biais d'une base de données enfreint-il vos ententes avec vos bailleurs de fonds ou les lois sur la protection des renseignements personnels?

Si votre organisation décide de se procurer une base de données, réfléchissez à comment vous allez:

- Maintenir le droit à la vie privée d'une femme d'un enfant ou d'un jeune et quelles sont les implications éthiques de l'utilisation d'une base de données
- Aborder les risques que posent les bases de données à la sécurité des femmes, des enfants et des jeunes
- Vous assurer que la mise en œuvre d'une base de données ne perpétue pas involontairement la violence. Votre base de données pourrait-elle aider les délinquants à commettre d'autres actes de violence, en interceptant des données par exemple, ou en y accédant sans autorisation?
- Expliquer les avantages directs pour les femmes, les enfants et les jeunes que vous desservez d'entrer leurs renseignements personnels dans une base de données
- Vous assurer que le personnel a le temps de mettre à jour la base de données
- Financer le coût d'installation initial et les mises à jour subséquentes

AVANTAGES DES BASES DE DONNÉES POUR LES ORGANISATIONS

Les organisations antiviolence choisissent une base de données pour tout une gamme de motifs. Les avantages comprennent:

- Les bases de données permettent aux organisations d'analyser les relations entre les données et de produire des rapports sur l'utilisation des services[5]
- Les bases de données sur les ressources éliminent le besoin de recréer des documents ou des ressources et offrent généralement des recherches par mots-clés qui fournissent des résultats rapides[6]

[5] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. Tiré de: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf
[6] National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. Tiré de: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

- Les bases de données offrent aux organisations l'avantage d'uniformiser leur méthode de collecte des données
- Les bases de données offrent aux organisations dispensant des services un système unique et la plupart du temps facilement accessible à l'ensemble des personnes utilisatrices

COLLECTE DE DONNÉES ET LOIS CANADIENNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

BC's Personal Information Protection Act: Un exemple

En raison d'une véritable possibilité d'atteinte à la sécurité des renseignements personnels, la collecte et le stockage inutiles de renseignements sur une base de données électronique peuvent accroitre les risques à la sécurité des femmes, enfants et jeunes qui subissent la violence. La majorité des fournisseurs de bases de données offrent des produits prêts à l'emploi qui peuvent entreposer plus de renseignements personnels concernant les récipiendaires de services que la quantité normalement conservée sur papier. Pour veiller à ne collecter que les renseignements nécessaires à la fourniture des services appropriés, les organisations antiviolence doivent *examiner soigneusement chaque champ de données* et travailler avec les fournisseurs à la personnalisation de la base de données en décidant quels champs «désactiver» ou «supprimer» pour des solutions moins invasives et respectueuses des lois sur la protection des renseignements personnels.

Les organisations antiviolence doivent:

- interroger le pourquoi de chaque champ dans une base de données
- se demander si le champ de données est nécessaire à la fourniture des services
- se demander si le champ pose des questions qui pourraient mettre à risque les femmes, les enfants et les jeunes en cas de fuite de données
- examiner et supprimer les champs qui ne sont pas conformes à leurs pratiques et leur mandat et qui peuvent avoir des incidences sur la responsabilité de l'organisation.

Par exemple, dans une base de données nationale, un champ de données pourrait demander d'inscrire toute **suspicion** d'enjeux de santé ou de santé mentale. Dans un tel cas, soulignons que les fournisseurs de services des organisations antiviolence n'ont pas toujours les connaissances et les antécédents professionnels requis pour évaluer les enjeux de santé ou de santé mentale des récipiendaires de services. De plus, ces données ne sont peut-être pas directement pertinentes aux services offerts et il n'existe peut-être pas de base concrète concernant cette condition «suspectée». Aux termes de la BC's *Personal Information Privacy Act*, les récipiendaires de services ont un droit d'accès, et à l'obtention d'une copie, de leurs dossiers, et peuvent également demander une révision, qui inclurait leurs dossiers sur bases de données. Le rapport de confiance entre les récipiendaires de services et le personnel des organisations antiviolence peut être rompu si la personne desservie s'aperçoit que son intervenant-e l'a

suspectée d'une maladie physique ou mentale et n'a pas abordé le sujet au cours du processus de fourniture de services. Les assignations à comparaitre sont un autre des risques encourus. Si le dossier d'une femme est requis par une tierce partie et subséquemment rendu public, la cliente «suspectée» de troubles de santé mentale ou physique peut subir de graves répercussions dans d'autres instances, comme devant le Tribunal de la famille dans ses décisions concernant la garde des enfants. Les organisations antiviolence et leur personnel peuvent faire l'objet de plaintes en matière civile ou être accusées d'atteinte à la vie privée en l'absence des compétences professionnelles requises pour établir ce type d'évaluation, et lorsque cette opinion cause préjudice aux récipiendaires de services.

Il est de bonne pratique pour les organisations antiviolence de ne collecter et stocker que les renseignements personnels des femmes, des enfants et des jeunes ***nécessaires*** à la fourniture de services, et seulement pour le temps nécessaire. Les lois provinciales, territoriales et fédérales sur la protection des renseignements personnels régissent les pratiques de gestion des dossiers de toutes les organisations antiviolence et fournissent également des lignes directrices sur l'utilisation des bases de données.

En Colombie-Britannique, la *Personal Information Protection Act* (PIPA) guide la collecte des renseignements personnels. Vous trouverez ci-dessous un tableau qui résume les exigences en matière de protection des renseignements personnels pour la majorité des organisations antiviolence sans but lucratif de la Colombie-Britannique. Se conformer à la PIPA fournit aux organisations antiviolence un cadre pour examiner la nécessité de divers champs dans leurs bases de données et pour réfléchir au processus de personnalisation avant d'utiliser une base de données «prête à l'emploi». Les organisations antiviolence ailleurs qu'en Colombie-Britannique sont encouragées à créer un tableau semblable en utilisant les lois de leur province ou territoire, ou les lois fédérales.

Selon la PIPA, C.B.:	Considérations à prendre en compte concernant les bases de données
Les organisations doivent obtenir le consentement informé des récipiendaires de services en vue de collecter, utiliser et/ou divulguer des renseignements personnels[7].	La loi prescrit l'obtention du consentement. Communiquez l'information suivante aux récipiendaires de services: • leurs renseignements personnels seront téléchargés dans une base de données électronique • qui a accès à cette base de données (spécialistes en TI, personnel, bénévoles) • où sont stockées leurs données

[7] Province de la Colombie-Britannique. (2013). Personal Information Protection Act. Tiré de: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

	• comment révoquer leur consentement et les risques associés à cette révocation Il est de bonne pratique que le consentement informé soit confirmé par écrit et limité dans le temps.
Les organisations doivent fournir des services même lorsque quelqu'un ne donne pas son consentement à la collecte et au stockage électroniques de leurs renseignements personnels. Les organisations ne doivent pas… comme condition pour fournir un service, exiger qu'une personne consente à la collecte de ses renseignements personnels[8].	Les organisations devraient avoir en place des politiques prévoyant l'éventualité où des récipiendaires de services refusent que l'on collecte leurs renseignements personnels et qu'on les entre dans une base de données. Le refus de voir ses renseignements personnels stockés dans une base de donnée électronique ne devrait pas entraîner un déni de services.
Sur demande, les organisations doivent fournir de l'information sur comment et pourquoi les renseignements sont utilisés et sur qui peut y accéder. Sur demande de récipiendaires de services actuels ou anciens, une organisation doit fournir les éléments suivants: • les renseignements personnels de l'individu qui sont sous contrôle de l'organisation • de l'information sur les façons dont les renseignements personnels… ont été et sont utilisés par l'organisation	• La base de données de l'organisation permet-elle d'imprimer les dossiers électroniques ou les renseignements personnels de récipiendaires de services ou de personnes qui participent à l'organisation sans mettre en péril d'autres renseignements stockés dans la base de données? • L'organisation est-elle dotée d'une politique régissant la façon dont elle utilise les renseignements personnels stockés dans la base de données? • Si les responsables de la base de données et les entreprises sous-traitantes qui hébergent les données de l'organisation (p.ex., stockage en nuage) ont accès à la

[8] Province de la Colombie-Britannique. (2013). Personal Information Protection Act. Tire de: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

• les noms des personnes et des organisations à qui les renseignements personnels… ont été divulgués[9]	base de données, s'assurer qu'elles sont incluses dans le formulaire de consentement qui énumère qui a accès à l'information électronique.
Les organisations doivent sécuriser les renseignements personnels. Les organisations doivent protéger les renseignements personnels sous leur garde ou leur contrôle en prenant des dispositions de sécurité raisonnables visant à prévenir l'accès, la collecte, l'utilisation, la divulgation, la copie, la modification, ou la destruction non autorisés, ou des risques semblables[10].	Il est de bonne pratique de collecter et de stocker **seulement** l'information nécessaire pour fournir le service qu'une femme, un enfant ou un jeune requiert pour le temps nécessaire. Si la base de données de l'organisation est connectée à internet, quelques questions se posent: • Les dossiers sont-ils cryptés à connaissance nulle? • Quelle est la longueur de votre clé de cryptage? • Qu'arrive-t-il si vos données sont «décryptées» par de tierces parties? • Votre organisation a-t-elle des logiciels pare-feu et anti-virus? • Votre organisation a-t-elle le budget pour maintenir des logiciels anti-virus et de sécurité? • Quelles sont vos politiques au cas où de tierces parties accèdent à vos dossiers, ou si le serveur de votre organisation est déplacé ailleurs? • De quels niveaux d'accès disposera le personnel? • Quels plans de sécurité avez-vous en place pour sauvegarder vos anciens disques durs ou en disposer?

[9] Province de la Colombie-Britannique. (2013). Personal Information Protection Act. Tiré de: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

[10] Province de la Colombie-Britannique. (2013). Personal Information Protection Act. Tiré de: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Les organisations doivent détruire les renseignements personnels dans un délai opportun. Les organisations doivent détruire les documents contenant des renseignements personnels, ou supprimer les moyens par lesquels les renseignements personnels peuvent être associés avec des individus en particulier, aussitôt qu'il est raisonnable d'assumer que: • l'objectif pour lequel ces renseignements personnels ont été collectés est périmé et leur rétention n'est plus nécessaire • la rétention n'est plus nécessaires à des fins juridiques ou à des fins d'affaires[11].	Les données informatiques peuvent souvent être recouvrées. Il est donc recommandé d'avoir: • une carte de tous les emplacements où les renseignements des récipiendaires de services sont stockés: ordinateurs, portables, tablettes, téléphone intelligents, téléphones, photocopieuses, scanners, centres de stockage en nuage, courriels, messages textes et médias sociaux • un plan pour détruire de manière permanente les renseignements personnels des récipiendaires de services sur tous les appareils • un plan pour savoir quand supprimer un dossier après sa fermeture et la fin de la période de rétention • une discussion avec des spécialistes en développement informatique: ○ est-il possible de supprimer un dossier de façon permanente, si votre organisation utilise toujours la base de données ○ comment le fournisseur de bases de données va-t-il garantir que les renseignements personnels des femmes sont supprimés de façon permanente de tous les lieux de stockage?

Autres considérations:

[11] Province de Colombie-Britannique. (2013). Personal Information Protection Act. Tiré de: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

- Les lois sur la protection des renseignements personnels et les données électroniques varient d'une province, d'un territoire et d'un pays à l'autre. Sachez que ces lois s'appliquent aux dossiers de votre organisation s'ils sont stockés dans une autre région autre que la vôtre, par exemple, sur un serveur de stockage en nuage. Si vos données sont stockées hors site, demandez au fournisseur de bases de données qui est propriétaire du site et quelles sont les lois qui s'appliquent.
- Ayez un plan au cas où votre base de données fasse l'objet d'une ordonnance du tribunal ou d'une assignation concernant la base de données en entier et un plan pour répondre à une ordonnance du tribunal ou une assignation d'un dossier individuel.
    - Comment allez-vous contester cette ordonnance du tribunal ou cette assignation en vue de protéger les renseignements personnels de l'ensemble des récipiendaires de services, de même que les renseignements opérationnels de l'organisation?
    - Comment allez-vous aviser les récipiendaires dont les renseignements personnels sont stockés dans votre base de données aux termes des lois sur la protection sur les renseignements personnels?
    - Comment allez-vous assurer la sécurité des femmes, des enfants et des jeunes si leurs noms, adresses, et autre renseignements personnels stockés dans une base de données par le personnel de votre organisation sont éventuellement violés par une personne non autorisée ou font l'objet d'une atteinte à la sécurité?

Atteintes à la vie privée et stockage des renseignements personnels

Selon le Commissariat à protection de la vie privée du Canada, une atteinte à la vie privée se définit comme la perte, l'accès non autorisé ou la communication par erreur de renseignements personnels. Cela peut se produire de multiples manières, incluant le vol, la perte ou le partage par erreur[12]. Les atteintes à la vie privée sont des conséquences de procédures organisationnelles déficientes ou de défaillances opérationnelles.

Les politiques et les formations en matière d'atteintes à la sécurité, la confidentialité et la vie privée des renseignements personnels vont aider le personnel antiviolence à comprendre pourquoi il ne faut collecter et stocker que les renseignements nécessaires à la livraison de services. Soyez au fait des responsabilités potentielles pour le personnel et l'organisation de la collecte d'un trop grand nombre de données. La reconnaissance des risques que pose le stockage électronique de renseignements pour la sécurité des femmes peut encourager une organisation à uniformiser sa méthode de collecte des renseignements et sa façon d'utiliser les bases de données. Avant la mise en place d'une base de données, les organisations doivent envisager la possibilité d'atteintes à la vie privée, qui peuvent s'avérer létales pour des femmes, des enfants et des jeunes qui fuient la violence ou subissent ses impacts. Les atteintes à la vie privée peuvent également coûter très cher à une organisation car elles peuvent donner lieu à des répercussions légales telles des plaintes portant sur la confidentialité et des protocoles que doit suivre une organisation en cas de fuite de données.

Cela dit, avant d'intégrer dans leur fonctionnement une base de données électronique, les organisations devraient savoir comment et où seront stockés les renseignements personnels collectés. La façon dont une base de données stocke les renseignements personnels de femmes, d'enfants et de jeunes est primordiale dans le choix du *type* de base de données. Celles-ci peuvent stocker les renseignements sur un serveur de l'organisation, ou sur internet par le biais d'une installation de stockage en nuage.

STOCKAGE DES DONNÉES

Considérations sur les divers types de stockage des données: a) Bases de données hébergées à distance et, b) Bases de données hébergées localement

A) Bases de données hébergées à distance

La majorité des bases de données les plus pertinentes pour les organisations antiviolence sont hébergées à distance. Leur principal avantage consiste à être accessible à partir de presque tous les appareils ayant une connexion internet. Stocker les renseignements personnels de femmes, d'enfants et de jeunes sur internet par l'entremise d'une installation de stockage en nuage pose un

[12] Commissariat à la protection de la vie privée du Canada. (2018). Atteintes à la vie privée. Tiré de: https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/atteintes-a-la-vie-privee/

éventail de risques à la sécurité des renseignements des femmes qui doivent être pris en considération, notamment:

- Le risque d'accès par internet de tierces parties non autorisées (parfois des pirates ou des publicitaires) aux dossiers des récipiendaires de services de votre organisation.
- Si une organisation souhaite acquérir une base de données hébergée à distance, les bases de données cryptées à connaissance nulle sont les plus sécuritaires. Toutefois, quelqu'un de l'extérieur pourrait quand même y accéder sans autorisation en empruntant, par exemple, le code d'identification, le mot de passe ou la clé de cryptage d'une employée.
- Si le personnel peut accéder à la base de données à l'extérieur du lieu de travail, il importe de prendre en compte les possibilités suivantes:
    - leur code d'identification et leur mot de passe sont entreposés sur des appareils publics et personnels connectés à internet, comme des portables, des ordinateurs et des téléphones
    - l'information peut être compromise par d'autres personnes accédant à l'ordinateur, ou
    - par une tierce partie observant quelqu'un du personnel entrer son code d'identification et son mot de passe.
- La possibilité que les portables, téléphones et tablettes soient égarés ou volés. Est-ce que les codes d'identification et les mots de passe sont stockés ou sauvegardés sur ces appareils?
- Certains fournisseurs de bases de données ont accès à celle de l'organisation pour résoudre d'éventuels problèmes techniques ou effectuer les mises à jour requises. Bien que cela puisse sembler un avantage de votre licence, la confidentialité des récipiendaires de services peut être compromise si l'entreprise peut accéder à votre base de données en tout temps sans restrictions. Idéalement, le personnel du fournisseur de bases de données ne devrait pas avoir le droit d'accéder aux renseignements personnels confidentiels de votre clientèle. En cas de transfert par le fournisseur de vos dossiers sur un nouveau système, ayez un plan de sécurité en place et avisez les récipiendaires de services avant de procéder au transfert.

B) Bases de données hébergées localement

Les bases de données hébergées localement stockent les renseignements personnels sur un serveur de l'organisation et sont accessibles sans avoir recours à internet. Alors que les bases de données hébergées localement sont l'une des options les plus sécuritaires, elles peuvent tout de même avoir des incidences sur la vie privée des femmes, des enfants et des jeunes du fait qu'elles sont difficiles à sécuriser. Bien connaître les options et les risques quant à la sécurité et la vie privée qu'entraîne l'utilisation de bases de données électroniques fait partie intégrante de la mise en place de mesures de sécurité raisonnables. Les éléments à prendre en considération dans le cas de bases de données hébergées localement comprennent:

- Si le serveur de votre organisation est connecté à internet, les renseignements personnels stockés dans votre base de données électronique sont vulnérables au piratage de votre réseau ou de votre ordinateur au moyen de cette même connexion.
- Qui a accès à l'espace où est entreposé le serveur de votre organisation? Est-ce que des bénévoles, membres du personnel, responsables de l'entretien, entreprises de services publics, résidentes, participantes ou autres fournisseurs de services peuvent accéder à l'endroit où est entreposé votre serveur? Est-ce que quelqu'un peut s'introduire dans le local où est entreposé votre serveur et le subtiliser?
- Votre organisation peut-elle payer pour le maintien du serveur, en plus de défrayer le renouvellement annuel de la licence? Les bases de données stockées sur le serveur d'une organisation nécessitent habituellement les services d'une personne spécialisé en TI pour mettre la base de données à jour, et s'assurer que les correctifs et les précautions de sécurité soient actualisés. Est-ce que des spécialistes en TI ont accès aux renseignements personnels des récipiendaires?
- Votre infrastructure de TI est-elle à jour et surveillée de près pour veiller à ce que toutes les mises à jour de sécurité soient réalisées, comme les pare-feu et les anti-virus?
- Si la base de données est stockée sur votre propre serveur, demandez-vous comment votre fournisseur y accède à des fins d'entretien.

Une note sur le stockage de données biométriques

L'identification ou authentification biométrique est une technologie qui utilise des aspects du corps humain (reconnaissance rétinienne, empreintes digitales, reconnaissance faciale, etc.) pour autoriser l'accès à un espace numérique. L'authentification biométrique est une technologie souvent invasive parce que les données collectées concernent le corps humain. Par comparaison aux numéros de téléphone et adresses, qui peuvent changer, les données biométriques sont irréversibles parce que ce sont des données physiques. Une atteinte aux bases de données où sont stockés des renseignements biométriques peut créer de nouveaux risques graves et irréversibles à la vie privée et la sécurité des femmes, enfants et jeunes récipiendaires de services et du personnel.

Certaines organisations envisagent l'utilisation de méthodes d'identification et d'authentification biométriques qui sont mises en marché avec une promesse de sécurité. Certaines bases de données offrent une option de stockage de renseignements biométriques. Quel que soit le produit qui requiert des renseignements biométriques (système de sécurité, téléphone intelligent ou base de données), les renseignements personnels et uniques d'un individu seront stockés «quelque part» et il est important de garantir leur confidentialité et leur sécurité.

Si les produits et les bases de données que votre organisation utilise ont la capacité de stocker des renseignements biométriques, posez-vous les questions suivantes:

- Ces renseignements sont-ils cryptés à connaissance nulle?[13]
- Comment pourrait-on intercepter des renseignements dans une base de données biométriques ou voler des renseignements personnels et/ou concernant l'identité?
- Qu'arrive-t-il lorsque des renseignements biométriques sont supprimés?
- Qu'arrive-t-il si la technologie biométrique accorde ou refuse l'accès à la mauvaise personne?

SÉCURITÉ INTÉGRÉE DÈS LA CONCEPTION

Avant d'utiliser une base de données, il est recommandé de procéder à un audit de vos infrastructures et systèmes actuels de TI. Considérez l'embauche d'une personne ou d'une entreprise de confiance spécialisée en TI pour tester la sécurité de votre réseau et de vos procédures de protection des renseignements. Un audit externe peut vous fournir une analyse en profondeur de vos points faibles et forts. Un audit peut révéler que les logiciels de sécurité doivent être mis à jour ou remplacés pour protéger au maximum les renseignements personnels de la clientèle. Voici une liste de suggestions tirées du document «Data Security Checklist to Increase Victim Safety & Privacy» du National Network to End Domestic Violence[14].

Minimiser la quantité de données collectées

De nombreuses bases de données «prêtes à l'emploi» ont la capacité de stocker une quantité exorbitante de renseignements pour chaque récipiendaire de services. Une collaboration entre le personnel de l'organisation antiviolence et le fournisseur de la base de données sur la personnalisation des champs de données permettra d'améliorer grandement la protection de la vie privée et de la confidentialité. La majorité offrent la possibilité de désactiver, désélectionner et effacer les champs inutiles à la réalisation du mandat de l'organisation. Minimiser la quantité de données collectées va amoindrir les risques à la sécurité des femmes et réduire la responsabilité de l'organisation et les risques de fuites de données.

Révisez les objectifs de votre organisation et/ou projet et évaluez votre processus de collecte des données en examinant les points suivants:

- Existe-t-il des possibilités moins invasives de mesurer les résultats et de simplifier l'admission?

---

[13] Le cryptage à connaissance nulle signifie que les fournisseurs de services ne connaissent rien des données que vous stockez sur leurs serveurs. Réf: Lam, Istvan. (2016). What is Zero-Knowledge Encryption? Tiré de: https://tresorit.com/blog/zero-knowledge-encryption/

[14] National Network to End Domestic Violence, Safety Net Project. (2008). Data Security Checklist to Increase Victim Safety & Privacy. Tiré de: https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5c016277575d1ff2db2060d3/1543594616517/NNEDV_DataSecurity_English08_access.pdf

- Comment les renseignements que vous prévoyez collecter pourraient-ils être mal utilisés en cas d'accès par des moyens légitimes et illégitimes?

Politiques sur les bases de données: développement, mise en œuvre et formation du personnel
Avant de mettre en place une base de données, les organisations doivent élaborer des politiques et procédures très claires qui mettent l'accent sur le respect de la vie privée dans la collecte, le stockage et l'élimination des données sensibles. Il est de bonne pratique pour les organisations de former tous leurs effectifs sur ces politiques et de réitérer régulièrement ces politiques lors des rencontres du personnel.

Les politiques concernant les bases de données devraient inclure[15]:

- Le contenu des dossiers, leur durée de vie et qui peut y accéder.
- Le type de renseignements qui pourront être entrés dans une base de données.
- Pour quel motif votre organisation collecte-t-elle les renseignements qu'elle stocke? Faites la démonstration d'un besoin précis ou d'une justification logique.
- Processus permettant aux femmes de refuser de participer, de se retirer du processus, ou de vérifier ou corriger leurs renseignements/dossiers.
- Procédures de collecte, de modification, d'utilisation et de divulgation de renseignements.
- Comment une personne peut-elle demander à voir son dossier ou modifier ses renseignements.
- Processus de destruction si les renseignements doivent être supprimés de façon permanente.
- Comment les renseignements personnels sont-ils stockés de façon sécuritaire pour la période requise aux termes des lois sur la protection de la vie privée.
- Processus de sélection, de formation et de vérification des antécédents des personnes ayant accès à des renseignements sensibles.
- À partir de quels appareils peut-on accéder à la base de données?
- Niveaux d'accès: qui peut accéder à quels renseignements, et comment l'accès peut-il être modifié ou révoqué?
- Procédures de protection contre l'utilisation ou l'accès non autorisés.
- Procédures en cas de plainte contre votre organisation pour atteinte à la vie privée.

Pour des exemples de politiques, voir «Use of Technology Policy Template Guide for BC's Prevention, Education, Advocacy, Counselling and Empowerment (PEACE) Programs for children and youth experiencing violence.» de la BCSTH

UTILISATION D'ANTI-VIRUS ET DE PARE-FEU

[15] National Network to End Domestic Violence, Safety Net Project. (2011). FAQs of Record Retention and Deletion. Tiré de: https://www.techsafety.org/retention

Si vous possédez un réseau de bureaux, il est recommandé d'utiliser des programmes anti-virus ou pare-feu. L'installation de logiciels anti-virus ou de pare-feu matériels sont d'importantes étapes de sécurité pour toute organisation possédant un accès internet. Toutefois, l'installation d'anti-virus et de pare-feu ne sont pas suffisants en soi pour protéger adéquatement les renseignements personnels des femmes, des enfants et des jeunes. Des mises à jour et des renouvellements devraient être planifiés sur une base régulière et, après consultation avec des spécialistes des TI, l'organisation devrait peut-être prendre d'autres précautions.

Utilisation de codes d'identification et de mots de passe pour tout le monde
Il est de bonne pratique pour chaque membre du personnel, bénévole, stagiaire et membre du conseil d'administration ayant accès à un ordinateur de l'organisation de posséder leur propre code d'identification et mot de passe. Ces dispositions permettent de savoir qui a accès au réseau et à la base de données d'une organisation. La gestion des mots de passe est un élément critique de la sécurité des données. L'utilisation de noms d'animaux de compagnie, de dates d'anniversaire ou de mots trouvés dans le dictionnaire devrait être interdite. Les mots de passe devraient être changés fréquemment et conservés en sécurité (pas sous le clavier de l'ordinateur ou scotchés sur l'écran). Un écran de veille activé par mot de passe pour le personnel ayant accès à des renseignements personnels aide à améliorer la sécurité des données quand elles et ils s'éloignent de l'ordinateur.

UTILISEZ LE CRYPTAGE
Le cryptage est la conversion de données sous une forme ne pouvant pas être facilement décodée par des personnes non autorisées. Le cryptage n'est pas la solution à tous les problèmes de sécurité; c'est une petit morceau d'une solution de sécurité complète. Le cryptage à connaissance nulle est l'option la plus sécuritaire. Il faut s'assurer auprès du fournisseur de bases de données que tous les renseignements entrés et stockés dans la base de données et dans les systèmes de sauvegarde sont cryptés à connaissance nulle. Si tel n'est pas le cas, renseignez-vous davantage au sujet de leur méthode de cryptage et des façons de décrypter les dossiers de votre organisation. Les organisations doivent avoir un plan en place au cas où leurs renseignements seraient «décryptés» par le fournisseur ou par une tierce partie.

NIVEAUX D'ACCÈS
Les niveaux d'accès permettent de déterminer qui aura accès à la base de données et de fixer le niveau d'accès pour chaque personne utilisatrice. Les niveaux d'accès doivent être personnalisés pour chaque membre du personnel, bénévole, stagiaire et membre du conseil d'administration ayant accès à la base de données. Est-ce que les gestionnaires, le personnel et les bénévoles n'ayant pas accès directement aux femmes, enfants et jeunes ont toutes et tous besoin du même niveau d'accès à la base de données? Le réglage du niveau d'accès en fonction des besoins peut améliorer la protection de la vie privée des récipiendaires de services.

Par exemple, la personne qui administre le système peut établir des niveau d'accès qui vont permettre à un petit nombre de membres du personnel d'accéder à tous les renseignements dans la base de

données, limitant celui des autres à leurs besoins. Limiter le nombre de personnes autorisées à consulter des renseignements personnels identifiables et sensibles peut aider les organisations à réduire les atteintes à la confidentialité. Dans la détermination du niveau d'accès, il convient de prendre en considération les risques à la sécurité au cas où les données seraient partagées à l'interne ou avec plusieurs autres organisations. Il est essentiel de relire les lois sur la protection des renseignements personnels fédérales et régionales qui stipulent qui peut avoir accès aux renseignements des femmes, enfants et jeunes qui accèdent à vos services.

Il est recommandé aux organisations de déterminer:

- Qui a besoin d'un accès aux renseignements?
- Quel est le niveau d'accès personnel approprié?
- Comment va-t-on procéder pour limiter l'accès aux personnes autorisées?
- Qui peut alimenter les dossiers (suivi des inscriptions aux dossiers)?
- Qui peut supprimer des renseignements?
- Comment les dossiers seront-ils détruits?

MISE À JOUR DU SYSTÈME OPÉRATIONNEL

Il est recommandé aux organisations d'avoir en place des politiques concernant les mises à jour régulières du système opérationnel et de nommer une personne chargée de télécharger régulièrement les dernières rustines et mises à jour pour vos systèmes opérationnels. Ceci est particulièrement important pour les bases de données hébergées localement parce que les rustines et les mises à jour devront être installées par le personnel, un-e spécialiste en TI ou un fournisseur de bases de données.

Sauvegarde des données

La plupart des bases de données ont un système de sauvegarde en place. Il est de bonne pratique de sécuriser les sauvegardes au même niveau de sécurité que la source originale.

Il est recommandé aux organisations de:

- Prévoir des systèmes de sauvegarde et de sécurité
- S'assurer que les données sauvegardées sont cryptées.
- Considérer faire affaire avec une entreprise de sécurité informatique pour leur demander d'évaluer la pénétrabilité/ sécurité de votre système et vous recommander des améliorations.

AUDIT DE GARANTIE DE LA QUALITÉ

Procéder à l'audit d'une base de données consiste à évaluer les renseignements collectés et supprimer toute information incorrecte. Au minimum, le personnel responsable des entrées au jour le jour ne devrait pas être chargé de l'audit. Les audits devraient inclure des échantillons aléatoires de renseignements collectés au sujet des récipiendaires de services pour aider à en évaluer la qualité et l'exactitude, et découvrir si des données inappropriées sont collectées et partagées.

FAITES APPEL À DES PROFESSIONNELS EN INFORMATIQUE
La plupart des organisations antiviolence sont sous-financées et n'ont pas les ressources nécessaires pour embaucher du personnel en TI à plein temps. Il est essentiel pour les organisations collectant des renseignements personnels et souvent sensibles de disposer d'un soutien technique professionnel. Pour limiter les coûts, une organisation peut:

- interroger d'autres organisations au sujet de leurs systèmes de collecte des données
- consulter d'autres organisations quant à la possibilité de contracter une entente leur permettant d'utiliser une copie de la base de données qu'elles ont personnalisée
- demander à votre association provinciale ou territoriale de maisons d'hébergement de vous aider dans vos démarches.

FORMATION CONTINUE
Pour maintenir la sécurité de votre base de données, il est recommandé de créer des occasions pour le personnel de participer à des formations spécifiques ou d'inviter des spécialistes qui viendront vous parler des lois sur la protection des renseignements personnels, de la sécurisation des données et des enjeux de sécurité des femmes. En raison du roulement élevé du personnel dans certaines organisations antiviolence, il est particulièrement important d'offrir des formations régulières pour maintenir la sécurité des renseignements personnels en vue de protéger la vie privée et la sécurité des femmes, enfants et jeunes avec qui votre organisation fait affaire.

Destruction des dossiers

Dans les provinces et territoires du Canada, diverses lois dictent la période durant laquelle des renseignements personnels doivent être retenus. Cela s'applique également aux renseignements stockés dans une base de données parce que les données collectées au sujet des récipiendaires de services sont considérées comme faisant partie de leur dossier personnel. Les organisations antiviolence doivent se conformer aux dispositions de rétention et de destruction inscrites dans les lois sur protection de la vie privée de leur province ou territoire.

La plupart des bases de données ont la capacité de stocker des renseignements jusqu'à ce qu'une organisation décide de cesser d'utiliser la base de données. Même alors, certaines bases de données stockées en nuage peuvent conserver les renseignements d'une organisation lorsque celle-ci cesse de l'utiliser. Les organisations peuvent réduire le risque d'éventuelles poursuites et fuites de données en collaborant avec un fournisseur à la personnalisation ou la conception d'une base de données conforme aux lois sur la rétention et la destruction de renseignements personnels dans leur province ou territoire.

Les organisations doivent s'assurer de:

- leur capacité de détruire les dossiers de manière permanente après la période requise
- leur capacité de supprimer les dossiers du serveur et de toute installation de stockage en nuage de manière permanente

- leur capacité de supprimer les sauvegardes de dossiers de manière permanente
- l'incapacité de la base de données ou du fournisseur de récupérer automatiquement les dossiers antérieurs des récipiendaires de services une fois qu'ils ont été détruits de manière permanente.

MAINTIEN DE LA CONFIDENTIALITÉ

Les politiques et pratiques d'utilisation d'une base de données devraient permettre aux femmes de refuser que l'on stocke leurs renseignements personnels dans une base de données électronique. Dans certaines provinces et certains territoires, les lois sur la protection des renseignements personnels énoncent clairement que les organisations doivent recevoir un consentement informé des récipiendaires de services avant de collecter et stocker leurs renseignements personnels. Si votre organisation utilise une base de données, le personnel doit obtenir des femmes un ***consentement écrit, informé et limité dans le temps*** reconnaissant qu'elles:

- consentent au stockage de leurs renseignements personnels dans une base de données électronique
- ont été informées sur qui a accès à leurs renseignements personnels
- connaissent les risques à la sécurité et la confidentialité associés avec cette méthode de collecte et de stockage des données.

Voici d'autres suggestions sur les éléments à inclure dans un formulaire de consentement informé. Ces points devraient également faire l'objet de discussions avec les récipiendaires de services:

- Qui sont les personnes ayant accès à la base de données électronique et combien sont-elles?
- Quels renseignements sont obligatoires ou facultatifs lors de la collecte de données?
- Dans combien d'endroits les données collectées seront-elles stockées?
- Quelles provinces, quels territoires ou quels pays hébergent leurs renseignements personnels?
- Quels sont les risques associés au stockage de leurs renseignements personnels dans une base de données?
- Quelles sont les obligations de l'organisation en cas de fuite de données?
- Comment et quand l'organisation va-t-elle supprimer/détruire leurs renseignements personnels?
- Quelles sont les politiques par rapport aux requêtes, assignations et ordonnances du tribunal présentées par de tierces parties?
- Qu'est-ce que l'organisation est prête à faire au nom des femmes en cas de fuite de données?

Le stockage d'informations sur une base de données électronique se déroule en plusieurs étapes et les renseignements peuvent se retrouver sur plusieurs serveurs dans diverses parties du monde. C'est pourquoi il peut s'avérer difficile de garantir que les dossiers ne seront pas violés ou compromis à un moment donné.

Étant donné la responsabilité des organisations utilisatrices de bases de données et les risques potentiels pour les femmes, les enfants et les jeunes, il importe d'examiner en profondeur les possibilités d'atteintes à la confidentialité que font peser les bases de données sur leur sécurité et leur vie privée. Les organisations ne devraient collecter que les renseignements nécessaires ***pour fournir les services durant une période donnée***. Les fournisseurs de bases de données font typiquement la promotion de la quantité de renseignements que leur base de données peut stocker en un seul endroit, comme des photos, des comptes Facebook, des noms et des adresses, le statut d'immigration ou ethnique, etc. La collecte de renseignements qui ne sont pas nécessaires à la livraison de services particuliers pose des risques à la vie privée, la confidentialité et la sécurité des femmes. Avant le lancement de votre base de données, collaborez avec la personne en charge du développement pour vous assurer que seuls les champs nécessaires sont inclus. Certains bailleurs de fonds d'organisations antiviolence n'exigent pas de renseignements personnels de la part des femmes pour leur permettre l'accès aux services – ces organisations desservent notamment des Jane Doe. D'autres bailleurs de fonds n'exigent pas l'ouverture d'un dossier pour accéder aux services. Chaque organisation antiviolence doit déterminer quel système de collecte des renseignements sera le plus efficace pour s'acquitter de son mandat et de sa mission de desservir adéquatement les femmes, les enfants et les jeunes qui forment sa clientèle.

Considérations de confidentialité dans le choix et la conception d'une base de données et dans l'élaboration de politiques régissant les bases de données organisationnelles:

- Qu'arrive-t-il si Citoyenneté et immigration Canada vous enjoint par ordonnance de divulguer votre base de données et découvre que votre organisation dessert des personnes n'ayant pas de statut d'immigrantes ou de réfugiées, ni de citoyenneté canadienne?

- Certaines bases de données prêtes à l'emploi demandent aux organisations de collecter des renseignements qui ne sont pas nécessaires à la livraison de services particuliers pour une période limitée. La collecte de renseignements non pertinents, qui n'ont rien à voir avec la situation, n'est pas conforme au mandat des organisations antiviolence, plutôt fondé sur la livraison de services de soutien confidentiels et appropriés.

- La collecte de renseignements biométriques n'offre pas nécessairement la flexibilité nécessaire pour protéger la confidentialité. Par exemple, si le système de sécurité de votre organisation demande aux résidentes de fournir leurs empreintes digitales pour accéder à votre maison d'hébergement, il existera quelque part une trace montrant qu'elles ont accédé aux services de votre organisation à une date spécifique.

- Est-ce que la décision d'une organisation antiviolence d'utiliser et stocker des renseignements biométriques ou des photos comme mécanisme de sécurité l'emporte sur la possibilité de mettre les femmes et leurs enfants à risque de «conséquences accidentelles?

- Quels sont les risques pour la sécurité des femmes si un ex-partenaire, ou l'associé d'un ex-partenaire, travaille pour le fournisseur de bases de données qui héberge leurs renseignements?

- Quels sont les risques pour la sécurité des femmes si un ex-partenaire, ou l'associé d'un ex-partenaire, travaille pour un organisme ayant accès aux données de votre organisation, tel un réseau régional de refuges pour sans abri par exemple?

- Considérez les graves répercussions sur la vie privée de la collecte d'une trop grande quantité de renseignements, tels les comptes de médias sociaux, des photos de récipiendaires de services et de leurs enfants, des numéros d'assurance-sociale, des informations sur le statut d'immigration, etc.

- Quelle est la vulnérabilité de votre base de données au vol, au piratage et à la violence? Est-ce que la base de données est hébergée sur un ordinateur connecté à internet?

- Si le tribunal vous enjoint de présenter le dossier d'une récipiendaire de services, avez-vous un moyen d'isoler les renseignements que vous devez nécessairement partager? Comment allez-vous veiller à ce que tous les autres dossiers dans la base de données ne soient pas compromis?

- Quelles sont les conséquences du fait que les renseignements personnels que vous entrez dans votre base de données électronique ne seront peut-être jamais complètement détruits?

Pour des modèles de formulaires, voir BCSTH «Legal Toolkit: General Information about Legal Issues and Court Matters in British Columbia» au https://bcsth.ca/publications/bcsth-legal-toolkit-general-information-about-legal-issues-and-court-matters-in-british-columbia/

QUESTIONS À POSER AUX FOURNISSEURS DE BASES DE DONNÉES

En communiquant avec les fournisseurs de bases de données il importe que les organisations antiviolence posent, au minimum, les questions suivantes au sujet de la protection de la vie privée dans leurs produits.

- Est-ce que la base de données possède la capacité de supprimer ou modifier des champs de données?
- Qui, hormis le fournisseur, aura accès aux renseignements stockés?
- Quelles sont les mesures de sécurité en place pour protéger les données et services de votre organisation? Par exemple:
    - Les données sont-elles cryptées et si oui, quel est le système de cryptage utilisé et qui possède la clé de cryptage?
    - Est-ce que la base de données est cryptée à connaissance nulle, ce qui signifie que personne en dehors de l'utilisateur peut accéder aux renseignements que vous stockez?
      Note: au moment de la rédaction du présent rapport et à partir des bases de données examinées pour cette recherche, le cryptage à connaissance nulle semble être la forme la plus sécuritaire de stockage de renseignements personnels.
- Est-ce que les données sont stockées au Canada?
- Est-ce que les données sont stockées dans un seul endroit?
- Il est de bonne pratique de s'assurer que le personnel du fournisseur de bases de données n'ait PAS ACCÈS aux renseignements d'une organisation. Souvent, les fournisseurs vont confirmer que leur personnel possède un accès, mais que leurs effectifs ont signé une clause de confidentialité. Il est important de poser des questions au fournisseur sur les mesures prises lorsque des membres de son personnel enfreignent cette entente de confidentialité.
- Si un fournisseur héberge les données d'une organisation, ce fournisseur peut-il refuser à l'organisation l'accès à ses propres renseignements en cas de fermeture de l'entreprise ou de survenue de problèmes techniques?
- Les organisations antiviolence ont-elles clarifié dans un contrat écrit qui est propriétaire des renseignements de votre organisation et qui peut y accéder, une fois les données stockées sur le serveur du fournisseur ou dans une installation de stockage en nuage.
- Le fournisseur est-il doté de politiques régissant ce qui arrive s'il reçoit une assignation ou une ordonnance du tribunal à produire vos dossiers?
    - Est-ce que le fournisseur va informer votre organisation de la réception d'une assignation ou d'une ordonnance du tribunal concernant vos dossiers?
    - Dans quels délais le fournisseur va-t-il vous contacter?
    - Quelles sont ses politiques dans ce domaine?

Aux termes des lois du Canada sur la protection de la vie privée, une fois les renseignements stockés dans la base de données, les organisations antiviolence sont responsables de la gestion des renseignements personnels contenus dans leurs dossiers, ainsi que des actions des spécialistes en développement des bases de données. Examinez le contrat du fournisseur avec un-e avocat-e en vue de vous assurer qu'il est conforme aux lois sur la protection de la vie privée de votre province ou territoire et qu'il inclut des protections en ce qui a trait au maintien de la vie privée et de la confidentialité des renseignements personnels des femmes, enfants et jeunes desservis par l'organisation antiviolence.

L'organisation américaine National Network to End Domestic Violence a produit une ressource intitulée «Selecting a Database» qui fournit des informations additionnelles pour guider les organisations antiviolence dans le choix et la mise en œuvre de systèmes de bases de données centrées sur les femmes. Pour plus d'information: https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/59e13157b1ffb6025f1804d1/1507930456484/NNEDV_SelectingDatabase_Chart_2011.pdf

EN GUISE DE CONCLUSION

L'installation d'une base de données électronique pour collecter et stocker les renseignements personnels des femmes et des enfants qui accèdent à des organisations antiviolence est une opération complexe. Les risques de fuite de données sont une possibilité omniprésente en cas de stockage électronique de renseignements personnels. Une atteinte à la confidentialité de renseignements personnels identifiables dans une organisation antiviolence peut mettre en danger les vies de femmes, d'enfants et de jeunes. Pour remédier à ces préoccupations, les organisations antiviolence devraient collecter le minimum de renseignements personnels nécessaires à la fourniture des services, et pour un temps limité. La collecte et le stockage de renseignements personnels auprès des récipiendaires de services ne doit pas leur causer de préjudices. Les femmes, les enfants et les jeunes qui font appel aux services d'organisations antiviolence leur font confiance quant à la protection de leurs renseignements personnels. Les femmes ont droit à toute l'information disponible concernant les possibilités d'atteintes à la sécurité et les risques à la vie privée qu'implique la collecte et le stockage électroniques de leurs renseignements personnels. L'obtention d'un consentement écrit, informé et limité dans le temps à la collecte et au stockage de renseignements personnels dans une base de données papier ou électronique est une pratique recommandée et régie par la loi dans la plupart des provinces et territoires au Canada.

Les préoccupations quant à d'éventuelles atteintes à la vie privée et à la sécurité des femmes, enfants et jeunes desservis par des organisations antiviolence doivent être prises en compte par les spécialistes en développement de bases de données avant l'exécution d'un contrat de mise en œuvre. Une organisation antiviolence qui décide d'installer une base de données électronique devrait considérer toutes les offres disponibles pour déterminer quelle option répond le mieux à ses besoins et laquelle est la plus conforme à ses objectifs et son mandat. La personnalisation d'une base de données fait partie intégrante des négociations et un contrat ne devrait jamais être conclu tant que ne sont pas remplies les conditions de l'organisation concernant la protection de la vie privée, la confidentialité et la sécurité. La majorité des fournisseurs conviennent que l'intégration d'une base de données ne peut se réaliser du jour au lendemain. Il importe de prévoir une période de temps suffisante pour permettre à l'organisation et au fournisseur de développer un plan précis de mise en œuvre et de personnalisation du produit en vue de veiller à ce que les renseignements personnels des récipiendaires de services soient en sécurité face aux risques actuels d'atteintes à la vie privée liés au stockage électronique de données.

Les organisations antiviolence doivent également intégrer un plan prévoyant les coûts indirects d'une base de données électronique. Même si la base de données est gratuite, il peut y avoir des coûts importants associés à l'infrastructure de TI, la recherche, les ressources humaines, le développement de politiques, la formation et les frais annuels. Tous ces coûts devraient être évalués durant le processus de détermination du besoin d'une base de données et de l'examen de sa conformité aux objectifs de l'organisation et de son mandat.

Disposer des fonds adéquats, et d'un accès aux ressources et au temps nécessaires pour créer un plan de mise en œuvre et assurer le suivi d'une base de données, vont faire la différence dans la protection de la vie privée des femmes, des enfants et des jeunes qui accèdent aux organisations antiviolence. Les ressources énumérées ci-dessous offrent aux organisations des renseignements additionnels pour leur permettre de faire des choix informés quant à la mise en œuvre d'une base de données électronique.

RESSOURCES

Lois sur la protection des renseignements personnels:
BC's Personal Information and Privacy Act:
http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01
Alberta's Personal Information and Privacy Act:
http://www.qp.alberta.ca/documents/Acts/P06P5.pdf
Loi sur la protection des renseignements personnels du Canada:
https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/atteintes-a-la-vie-privee/
Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE):
https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/

Infonuagique:
LPRPDE: L'Infonuagique pour les petites et moyennes entreprises:
https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie-et-vie-privee/protection-de-la-vie-privee-en-ligne/infonuagique/gd_cc_201206/
PIPA et LPRPDE:
Lignes directrices pour l'infonuagique:
https://www.oipc.bc.ca/guidance-documents/1437

Respect de la LPRPDE:
Conformité à la LPRPDE et outils de formation:
https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/conformite-a-la-lprpde-et-outils-de-formation/
Consulter vos renseignements personnels:
https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/acces-aux-renseignements-personnels/consulter-vos-renseignements-personnels/

Atteintes à la vie privée:
LPRPDE:
Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité:
https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/
PIPA:
Atteintes à la vie privée: Outils et ressources:
https://www.oipc.bc.ca/guidance-documents/1428

Information sur la sécurité technologique:
Sécuriser les renseignements personnels: Un outil d'autoévaluation pour les organisations: https://www.oipc.bc.ca/guidance-documents/1439

Information sur les bases de données pour organisations antiviolence:
Choisir une base de données:
https://nnedv.org/mdocs-posts/selecting-a-database/ ou https://www.techsafety.org/selecting-a-database/

RÉFÉRENCES

Lam, Istvan. (2016). What is Zero-Knowledge Encryption? Tiré de: https://tresorit.com/blog/zero-knowledge-encryption/

National Network to End Domestic Violence, Safety Net Project. (2008). Data Security Checklist to Increase Victim Safety & Privacy. Tiré de: https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5c016277575d1ff2db2060d3/1543594616517/NNEDV_Data

National Network to End Domestic Violence, Safety Net Project. (2011). FAQs of Record Retention and Deletion. Tiré de: https://www.techsafety.org/retention

National Network to End Domestic Violence, Safety Net Project. (2011). Selecting A Database. Tiré de: http://nnedv.org/downloads/SafetyNet/OVW/NNEDV_SelectingDatabase_Chart_2011.pdf

Commissariat à la protection de la vie privée du Canada. (2018). Atteintes à la vie privée. Tiré de: https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/atteintes-a-la-vie-privee/

Commissariat à la protection de la vie privée du Canada. (2016). Le gouvernement fédéral et vos renseignements personnels. Tiré de: https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/votre-droit-a-la-vie-privee/le-gouvernement-federal-et-vos-renseignements-personnels/

Province de Colombie-Britannique (2013). Personal Information Protection Act. Tiré de: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01