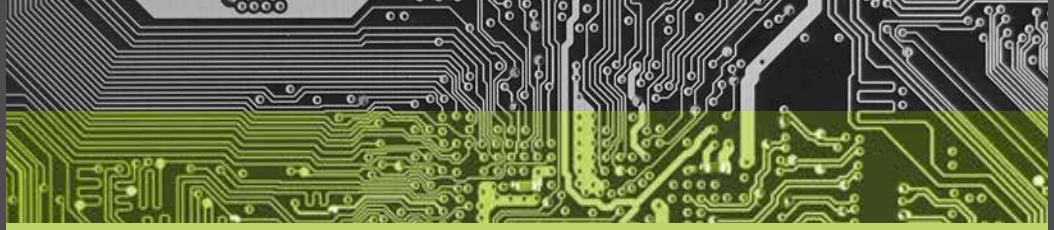

MARS 2018

FEUILLE-INFO
SUR LA TECHNOLOGIE

Comment se débarrasser des supports électroniques

La présente feuille-info contient des directives à l'intention des institutions du secteur public et des dépositaires de renseignements sur la santé de l'Ontario sur la destruction sécurisée de renseignements personnels au moment de se débarrasser de supports électroniques.

OBLIGATIONS JURIDIQUES

La *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*), son équivalent s'appliquant au palier municipal, la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (*LAIMPVP*) et la *Loi sur la protection des renseignements personnels sur la santé* (*LPRPS*) obligent les institutions et les dépositaires de renseignements sur la santé (les « dépositaires ») à prendre des mesures raisonnables pour protéger les renseignements personnels, y compris les renseignements personnels sur la santé, de leur collecte jusqu'à leur destruction.

La question de savoir si les mesures prises sont raisonnables ou non repose sur la situation. Dans tous les cas, vous devez détruire les renseignements de manière à ce qu'ils ne puissent pas être reconstitués ou récupérés.

Le présent document s'applique aux supports électroniques contenant des renseignements personnels qui seront jetés, recyclés, réutilisés ou mis à la disposition de personnes de l'extérieur de l'organisation, et notamment aux supports suivants :

- les supports magnétiques (comme les disques rigides et les bandes magnétiques);
- les supports électroniques (comme les disques électroniques, les clés USB et les cartes mémoire);

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

- les appareils mobiles (comme les téléphones intelligents et les tablettes);
- les disques optiques (comme les CD, les DVD et les disques Blu-ray).

L'IMPORTANCE DE LA DESTRUCTION SÉCURISÉE

Si elle néglige de protéger les renseignements personnels, votre organisation pourrait enfreindre la loi, s'exposer à des risques financiers et autres et ternir sa réputation. L'accès non autorisé à des renseignements personnels sauvegardés sur support électronique ou la divulgation inappropriée de ces renseignements est une atteinte à la vie privée qui peut se révéler lourde de conséquences pour les personnes concernées.

POINTS À RETENIR POUR ASSURER LA DESTRUCTION SÉCURISÉE DES RENSEIGNEMENTS

Pour assurer la destruction sécurisée des renseignements numériques, il faut savoir :

- qu'il ne suffit pas de supprimer des fichiers ou de formater un disque pour assurer la destruction sécurisée;
- qu'il faut employer une méthode adaptée au support en question;
- qu'il pourrait être nécessaire d'acheter un logiciel ou un dispositif spécial;
- que certains logiciels ne fonctionnent pas si le support est endommagé.

La présente feuille-info donne un aperçu des moyens d'assurer la destruction sécurisée des renseignements sauvegardés sur des supports électroniques. Elle ne présente pas de conseils pratiques détaillés. En tant qu'institutions et dépositaires, vous devez consulter vos conseillers en informatique pour mettre sur pied un processus efficace de destruction sécurisée afin de respecter les lois ontariennes sur la protection de la vie privée.

MÉTHODES DE DESTRUCTION SÉCURISÉE

Afin de détruire des renseignements personnels de façon sécurisée, vous devez agir sur le support sur lequel sont sauvegardés ces renseignements sous forme numérique. Il existe deux moyens de détruire des renseignements numériques de façon sécurisée :

- détruire le support lui-même;
- écraser les renseignements sauvegardés sur le support.

La meilleure méthode à employer repose sur le support en question. Soulignons que certains appareils, comme les imprimantes, les télécopieurs et les téléphones intelligents, peuvent contenir plusieurs types de supports, chacun nécessitant une méthode différente de destruction des renseignements.

La destruction matérielle du support constitue la méthode la plus draconienne de s'assurer que les renseignements ne pourront être récupérés. Grâce à des outils et à des services spécialisés, il est possible de désintégrer, d'incinérer ou de pulvériser appareils et disques. Les supports magnétiques peuvent aussi être *démagnétisés* par l'application d'un champ magnétique puissant qui supprime les renseignements sauvegardés. La démagnétisation, comme les autres méthodes de destruction matérielle, rend le support magnétique inutilisable, mais il permet de détruire de façon sécurisée tous les renseignements personnels sauvegardés.

L'écrasement (parfois appelé « nettoyage ») consiste à sauvegarder des données nouvelles et non délicates sur les renseignements à détruire. Il s'effectue au moyen d'un logiciel spécial, de différentes façons, selon le support. Par exemple, certains appareils mobiles sont dotés d'un logiciel d'écrasement spécialisé qui permet de détruire de façon sécurisée les renseignements qui y sont sauvegardés. Pour la plupart des supports magnétiques, par contre, il faut généralement utiliser un logiciel externe. Il est important de choisir une méthode et un outil d'écrasement adaptés au support en question.

L'écrasement est impossible si l'appareil ou le support est endommagé ou ne peut plus recevoir de données (p. ex., s'il s'agit d'un disque optique), ou s'il ne peut être effectué partout sur le support où des renseignements ont été sauvegardés. Il peut être difficile d'effectuer un écrasement sur des disques électroniques (plutôt que sur un disque magnétique) car ils sauvegardent les données de façon très différente. C'est pourquoi, en règle générale, l'écrasement n'est pas recommandé pour les disques électroniques.

L'effacement cryptographique est un type particulier d'écrasement qui remplace les données par d'autres données faisant l'objet d'un chiffrement fort, ce qu'on pourrait appeler l'effacement par chiffrement. Une fois les données chiffrées et les clés cryptographiques supprimées de façon sécurisée, les renseignements personnels sont irrécupérables. Cette méthode a toutefois pour inconvénient qu'il peut être difficile de confirmer la suppression sécurisée par l'inspection du support, car il n'y a aucun moyen de vérifier que les clés cryptographiques ont été effectivement supprimées.

La suppression de fichiers *n'est pas* un moyen acceptable de détruire des renseignements de façon sécurisée. Les fonctions de suppression de base ne détruisent pas les données de façon sécurisée, car lorsqu'un fichier est supprimé dans un ordinateur personnel, par exemple, seul le pointeur ou le lien menant à l'emplacement du disque où se trouvent les

données est supprimé. Les données elles-mêmes subsistent et ne sont pas détruites.

Le formatage du support *n'est pas* non plus un moyen acceptable de détruire des données de façon sécurisée. Comme la suppression de fichier, le formatage d'un disque dur ou d'une clé USB efface uniquement les pointeurs menant à l'emplacement où les données sont sauvegardées. Les données elles-mêmes subsistent et ne sont pas détruites.

Le tableau suivant résume les méthodes de destruction pour différents appareils et supports.

Supports	Recommandations	Aspects à envisager
Supports magnétiques (disques durs internes et externes, bandes magnétiques)	Écrasez les données à trois reprises **ou** Utilisez un démagnétiseur pour supprimer les propriétés magnétiques des données sauvegardées. Le support deviendra inutilisable en permanence. **ou** Détruisez le support	Vous aurez peut-être besoin d'outils spéciaux pour écraser les données se trouvant dans des zones cachées ou réservées Il peut être acceptable d'écraser les données une seule fois si vous comptez détruire le support Les supports magnétiques peuvent être désintégrés, incinérés ou pulvérisés
Supports électroniques (disques électroniques, clés USB, cartes mémoire)	Détruisez le support	Les techniques d'écrasement ne permettent pas de détruire de façon sécurisée les données sauvegardées sur les disques électroniques et cartes mémoire Les disques électroniques doivent être détruits par désintégration, incinération ou pulvérisation
Appareils mobiles (téléphones intelligents, tablettes)	Enlevez ou détruisez tout support électronique amovible **et** Écrasez les autres données sauvegardées dans l'appareil en effectuant une réinitialisation des paramètres d'usine par défaut conformément aux directives du fabricant	Après la réinitialisation des paramètres d'usine, vous devriez vérifier manuellement à différents endroits dans l'appareil pour vous assurer que toutes les données ont été détruites
Disques optiques (CD, DVD, disques Blu-ray)	Détruisez le disque	Enlevez les couches des disques optiques qui contiennent les données au moyen d'une meuleuse, ou détruisez les disques par incinération, déchiquetage ou pulvérisation

PROGRAMME DE DESTRUCTION DE DONNÉES

La destruction est une étape importante du cycle de vie de l'information, au même titre que les autres activités de gestion de l'information. Certaines conditions doivent être réunies pour assurer l'efficacité d'un programme de destruction des données.

Votre organisation doit disposer de politiques et de procédures de conservation et d'élimination de l'information. Elle doit aussi désigner une personne qui sera chargée d'assurer la tenue à jour de ces politiques et procédures et d'assurer la formation de tout le personnel.

Votre organisation devrait connaître la catégorie et l'emplacement de ses fonds de renseignements et des copies, y compris les copies de sécurité, et savoir à quel point ils sont délicats. Elle devrait également être en mesure d'identifier et de localiser tous les supports contenant des renseignements numériques.

VÉRIFICATION ET DOCUMENTATION

La destruction sécurisée de renseignements numériques doit être vérifiée. Pour ce faire, vous pouvez adopter des procédures organisationnelles aux fins de la vérification du processus de destruction, de l'efficacité du matériel ou des logiciels utilisés ainsi que des résultats.

Les institutions assujetties à la *LAIPVP* doivent tenir un relevé des renseignements personnels qui ont été détruits et de la date de destruction[1]. Les institutions municipales et les dépositaires sont encouragés à tenir des relevés semblables.

FOURNISSEURS EXTERNES

En tant qu'institutions et dépositaires, vous pouvez faire appel à des fournisseurs externes pour détruire vos renseignements numériques et supports de stockage. Nous vous recommandons de choisir un fournisseur de services réputé et de voir à ce que le contrat comprenne au moins les aspects suivants :

- modalités de vos rapports avec le fournisseur;
- obligations claires en matière de destruction sécurisée des renseignements;
- méthodes de destruction;
- certification de destruction une fois celle-ci effectuée;
- modalités d'inspection du processus de destruction;
- formation appropriée des employés responsables;
- restrictions touchant la sous-traitance;

1 R.R.O. 1990, Règl. 459, par. 6 (1).

- délais de destruction des documents;
- entreposage sécurisé en attendant la destruction.

RENSEIGNEMENTS SUPPLÉMENTAIRES

Pour obtenir des précisions et conseils sur la destruction des renseignements et documents numériques, consultez les documents suivants :

- CIPVP et National Association for Information Destruction (NAID), **Get Rid of it Securely to keep it Private – Best Practices for the Secure Destruction of Personal Health Information** (octobre 2009)
- Feuille-info n° 10 du CIPVP, **La destruction sécurisée de renseignements personnels** (décembre 2005)
- National Institute of Standards and Technology (NIST), **Special Publication 800-88, Guidelines for Media Sanitization** (décembre 2014)
- Gouvernement de l'Ontario, **NTI-GO 25.20 : Pertes par élimination et rapports d'incidents d'appareils informatisés et de supports de stockage numérique** (en anglais seulement) (mars 2014)
- Centre de la sécurité des télécommunications Canada (CSTC), **Ligne directrice sur la sécurité de la technologie de l'information (ITSG-06) - Effacement et déclassification des supports d'information électroniques** (juillet 2006)

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario