Commissaire à l'information et à la protection de la vie privée de l'Ontario

Feuille-info

Numéro 12
Mai 2007

Le chiffrement des renseignements personnels sur la santé dans les appareils mobiles

Le paragraphe 12 (1) de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (*LPRPS*) oblige les dépositaires de renseignements sur la santé à prendre des mesures qui sont raisonnables dans les circonstances pour veiller à ce que les renseignements personnels sur la santé dont ils ont la garde ou le contrôle soient protégés contre le vol, la perte et une utilisation ou une divulgation non autorisée et à ce que les dossiers qui les contiennent soient protégés contre une duplication, une modification ou une élimination non autorisée.

Le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario est conscient du fait que la prestation de soins de santé pourrait nécessiter l'utilisation de renseignements personnels sur la santé hors du lieu de travail, et que dans bien des cas, il est plus efficace de transporter et d'utiliser ces renseignements sous forme électronique. Or, même si les documents électroniques sont faciles à utiliser et à transporter, il demeure important de déplacer le moins possible de données de la sorte.

Les appareils mobiles comme les ordinateurs portables, les assistants numériques et les clés à mémoire flash sont souvent perdus ou volés; les dépositaires doivent donc veiller à chiffrer les renseignements personnels sur la santé qui sont sauvegardés dans ces appareils. Lorsque le chiffrement est effectué correctement, il permet d'éviter la divulgation de renseignements personnels sur la santé, et les documents électroniques ainsi chiffrés sont plus faciles à protéger que les documents sur papier pendant le transport.

La présente feuille-info est destinée aux dépositaires de renseignements sur la santé qui sauvegardent des renseignements personnels sur la santé dans des appareils mobiles, mais elle s'applique également à toute personne qui utilise ces appareils et y enregistre des renseignements personnels. Si vous avez besoin de précisions concernant l'interprétation de ces directives, veuillez consulter un expert en sécurité informatique afin de déterminer comment la présente feuille-info s'applique aux renseignements dont vous avez la garde. Pour chiffrer des données, il suffit dans bien des cas d'installer un logiciel simple et d'assurer une bonne gestion des clés du système.

J'utilise un mot de passe d'accès. N'est-ce pas suffisant?

Non, il est inacceptable d'utiliser uniquement un mot de passe d'accès pour protéger les renseignements personnels sur la santé sauvegardés dans des appareils qui risquent d'être perdus ou volés. Un mot de passe « fort » peut empêcher les tentatives d'accès superficielles, mais se révéler insuffisant pour contrer un voleur qui s'y connaît bien. Les mots de passe forts présentent généralement les caractéristiques suivantes :

- Ce ne sont pas des mots que l'on trouve dans le dictionnaire;
- Ils se composent à la fois de lettres, de chiffres et de symboles;
- Ils comportent au moins huit caractères, et de préférence 14 caractères ou plus.

Par exemple, « **OuvreToi** » est un mot de passe faible parce qu'il se constitue de mots que l'on trouve dans le dictionnaire. Par contre, vous pourriez mémoriser la phrase « mon anniversaire est le 21 octobre et j'ai 25 ans » pour obtenir le mot de passe fort « **Mael21o&j25** ». Comme il est parfois difficile de se rappeler des mots de passe forts, les gens créent souvent des mots de passe faibles. En outre, même les mots de passe forts peuvent être écrits, volés, partagés, obtenus par piratage ou cassés au moyen de logiciels faciles à obtenir sur le marché.

Qu'est-ce que le chiffrement?

Le chiffrement est un processus qui permet de transformer du texte ou des données ordinaires, appelés « texte en clair », en une série inintelligible et apparemment aléatoire de symboles appelée « texte chiffré ». Ce processus est régi par une « clé » numérique qui permet d'accéder aux données chiffrées. Cette clé peut être :

- une chaîne de caractères; par exemple, un mot de passe « fort » qui n'est pas un mot de passe d'accès car il existe des méthodes bien connues permettant de casser ces mots de passe;
- un objet comme une clé à mémoire flash ou une clé d'accès USB;
- un élément personnel comme votre empreinte digitale ou votre signature.

Sans cette clé, les données sont illisibles. Par exemple, l'expression « texte ordinaire » pourrait devenir « ~Sš£WÕN3@ƒ » après chiffrement. L'efficacité du chiffrement repose sur la norme de chiffrement et la force de la clé utilisée.

Quelles sont les options parmi lesquelles je peux choisir?

Le chiffrement des données dans les appareils mobiles peut s'effectuer de différentes façons.

Chiffrement complet du disque dur

Il est possible de chiffrer la totalité d'un disque dur; cette solution est privilégiée pour les nouveaux systèmes et devrait l'être également pour tout nouvel appareil mobile. L'achat de nouveaux systèmes représente peut-être d'ailleurs le moyen le plus facile d'implanter le chiffrement des données. Plusieurs entreprises vendent également des logiciels permettant le chiffrement complet du disque dur. Pour connaître les possibilités qui s'offrent à vous, recherchez l'expression « chiffrement complet » sur le Web ou parlez-en à un fournisseur. En règle générale, l'installation sur un ordinateur portable se fait aussi facilement que s'il s'agissait de n'importe quel autre logiciel.
Le chiffrement complet du disque dur représente probablement la solution la plus sécuritaire pour les dépositaires de renseignements sur la santé qui jugent devoir sauvegarder des renseignements personnels sur la santé dans des appareils mobiles.

Chiffrement de disque virtuel

Un disque « virtuel » est un fichier créé sur un disque existant. Le logiciel chiffre le fichier et le traite comme un disque distinct. Pour ce faire, il faut généralement acheter et installer un logiciel de disque virtuel ou de clonage de disque. L'accès au disque virtuel chiffré nécessite généralement un mot de passe fort qui n'est pas un mot de passe d'accès. Sans ce mot de passe et sans logiciel de chiffrement, le disque virtuel est indéchiffrable.

Le disque virtuel pourrait être la seule option réaliste sur les assistants numériques, qui ne permettent pas nécessairement le chiffrement complet. Il se révèle également utile sur les ordinateurs portables moins récents. Cependant, comme de nombreux systèmes ou logiciels créent automatiquement des fichiers temporaires ou de sauvegarde, le chiffrement virtuel n'est efficace que si ces fichiers, qui ne sont pas chiffrés au départ, sont eux-mêmes chiffrés ou supprimés après usage.

Chiffrement d'un dossier ou d'un répertoire

Les systèmes d'exploitation actuels sont dotés de certaines fonctions de chiffrement :

- Si vous avez un système Microsoft Windows XP, vous pouvez dans certains cas cliquer avec le bouton droit de la souris sur un dossier puis sur le bouton « Options avancées » à l'onglet « Général ». Sélectionnez « Crypter le contenu pour sécuriser les données » afin d'actionner le chiffrement.

- Si vous avez un système Apple OS X, vous pouvez chiffrer votre dossier « Départ » en activant « FileVault » dans l'onglet « Sécurité » des « Préférences Système ».

Ces options sont faciles à utiliser, mais étant donné qu'elles sont verrouillées au moyen du mot de passe d'accès de l'utilisateur, elles procurent une protection limitée qui ne suffit pas, à elle seule, pour les renseignements personnels sur la santé. Les données sont vulnérables car une personne y aura accès si elle obtient le mot de passe.

Chiffrement d'un appareil de stockage portatif

Au lieu d'un ordinateur portable, on peut également sauvegarder des renseignements personnels sur la santé dans un appareil de stockage portatif, comme une clé à mémoire flash. Les lecteurs de musique portables et les assistants numériques sont parfois dotés de cette fonctionnalité. Ces appareils portatifs sont toutefois faciles à perdre, de sorte qu'il est encore plus important de chiffrer les données. Comme pour les disques durs, il est possible de chiffrer tout l'appareil ou bien la partie qui contient des renseignements personnels sur la santé. Si vous avez acheté un logiciel en vue de créer un disque virtuel, tel qu'expliqué plus haut, il est possible que vous puissiez vous en servir pour chiffrer votre appareil de stockage portatif.

Chiffrement d'entreprise

La présente section est destinée aux dépositaires de renseignements sur la santé qui sont responsables d'un grand nombre d'appareils, qu'il s'agisse d'ordinateurs portables, d'assistants numériques ou d'appareils de stockage portatifs. Il ne serait peut-être pas réaliste de s'en remettre aux utilisateurs pour sélectionner et installer l'une ou l'autre des options précédentes. Il existe des solutions d'entreprise qui permettent aux dépositaires d'appliquer des normes de chiffrement sur tous les appareils qui relèvent d'eux. Vous pouvez chercher sur le Web les expressions « prévention des fuites de données », « protection contre la perte de données » ou « protection des systèmes d'extrémité », ou des expressions semblables, et vous trouverez bon nombre de possibilités, ou vous pouvez en parler à votre fournisseur. Certains outils font eux-mêmes le chiffrement ou fonctionnent de concert avec un outil de chiffrement déjà installé pour appliquer les politiques d'entreprise.

Dans une grande organisation, on ne peut surestimer l'importance d'une formation adéquate et de la création d'une culture de la vie privée. À moins de recevoir l'appui solide de la direction et d'être accepté par le personnel, un programme de chiffrement éventuel connaîtra l'échec.

Normes de chiffrement

Au moment où était rédigée la présente feuille-info, la norme privilégiée pour la sauvegarde sécurisée des données était l'AES, ou Advanced Encryption Standard. Elle comporte plusieurs versions, dont la force repose sur la longueur de la clé. L'AES-128 est suffisante, mais l'AES-192 et l'AES-256 sont beaucoup plus fortes. Comme les normes de chiffrement sont en évolution constante, les dépositaires doivent s'assurer que celle qu'ils utilisent répond aux normes généralement reconnues. Les dispositifs de chiffrement qui sont installés doivent être vérifiés et mis à jour régulièrement au besoin. En cas de doute, adressez-vous à un expert reconnu en sécurité.

Centres de sauvegarde

De nombreuses entreprises font des copies de sécurité de leurs données sur des bandes magnétiques ou d'autres supports, qu'elles entreposent à distance, hors de leur centre de traitement. En règle générale, les données ne sont pas transmises; les supports sont acheminés par voie routière vers les centres de sauvegarde. Les dépositaires de renseignements sur la santé doivent être conscients du risque de perte et veiller à chiffrer les données ou à les protéger au moyen d'autres méthodes, pour éviter que ces renseignements, qu'ils ont protégés dans leurs ordinateurs portables, ne soient révélés lors de la perte de bandes de sauvegarde non chiffrées.

Conclusion

La commissaire a déclaré que la perte ou le vol éventuel d'un appareil mobile ne sera pas considéré comme une atteinte à la vie privée si des mesures de sécurité suffisantes ont été mises en œuvre pour assurer la protection des renseignements personnels sur la santé. Grâce au chiffrement adéquat des données, les dépositaires pourraient gagner temps et argent en se soustrayant aux exigences de la *Loi* relatives aux avis et éviter une atteinte peut-être irréparable à leur réputation en cas de vol ou de perte de renseignements personnels sur la santé. Surtout, les particuliers concernés n'auraient plus l'angoisse d'apprendre que leurs renseignements personnels sur la santé ont été perdus ou volés.

Aide-mémoire pour le chiffrement

- ✓Je sauvegarde le moins possible de renseignements personnels sur la santé dans des appareils portables (et de préférence aucun renseignement permettant d'identifier les personnes concernées).
- ✓Je supprime les renseignements personnels sur la santé sauvegardés dans tous les appareils portables dès que je n'en ai plus besoin.
- ✓Je sais quels sont les renseignements personnels sur la santé qui sont sauvegardés dans chacun de mes appareils portables.
- ✓J'ai activé le système de chiffrement de mon système d'exploitation.
- ✓J'ai acheté un système doté d'un dispositif de chiffrement complet du disque dur.

  OU

- ✓J'ai acheté un logiciel permettant de chiffrer tout le disque dur de mon ordinateur portable ou de mon assistant numérique ou de créer un disque virtuel chiffré.
- ✓Si j'utilise des appareils de stockage portatifs comme des clés à mémoire flash, j'achète des clés avec dispositif de chiffrement, ou j'installe un logiciel de chiffrement avant de m'en servir pour sauvegarder des renseignements personnels sur la santé.
- ✓Si je protège des données chiffrées au moyen d'un mot de passe, j'utilise un mot de passe fort ET différent de celui dont je me sers pour accéder à mon ordinateur.

- ✓Je ne prends jamais note de mon mot de passe.
- ✓Je ne donne mon mot de passe à personne.
- ✓Si je n'utilise pas de chiffrement complet du disque dur, je peux déterminer l'emplacement de TOUS les renseignements personnels sur la santé sur mon système.
- ✓Je sauvegarde des renseignements personnels sur la santé uniquement sur le disque chiffré.
- ✓Je m'assure régulièrement que mes politiques en matière de chiffrement sont appliquées et respectées.

Solutions

Le CIPVP reconnaît que les personnes chargées de la protection des renseignements personnels sur la santé ne connaissent peut-être pas très bien les logiciels de chiffrement. Voici une liste de quelques solutions en vente sur le marché. Nous ne recommandons aucune de ces solutions en particulier, mais nous avons tenté de donner en exemple des sociétés représentatives des diverses solutions que l'on peut trouver. Soulignons que cette technologie évolue rapidement, et qu'une solution qui est perfectionnée aujourd'hui pourrait être dépassée demain.

Solution	Description	Site Web
CryptoMill	CryptoMill propose une solution de sécurité d'extrémité d'entreprise, y compris le chiffrement, avec son produit SeaHawk.	http://www.cryptomill.com
PGP	PGP propose un éventail de solutions en matière de chiffrement, y compris le chiffrement complet de disques durs.	http://www.pgp.com
TrueCrypt	Logiciel répandu à code source ouvert permettant de créer des disques virtuels ou d'assurer le chiffrement complet de disques durs sur des systèmes Windows ou Linux.	http://www.truecrypt.org
Vontu	Vontu fournit des solutions pour prévenir la perte de données d'entreprise, y compris l'application de politiques de chiffrement.	http://www.vontu.com
WinMagic	WinMagic procure un certain nombre de solutions en matière de chiffrement, y compris les logiciels SecureDoc Hard Disk Encryption et SecureDoc Mobile Edition.	http://www.winmagic.com

Feuille-info

est publié par **le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.**

Pour nous faire part de vos observations, nous informer d'un changement d'adresse ou pour que votre nom soit ajouté à la liste d'envoi, veuillez communiquer avec :

Service des communications
Commissaire à l'information et
à la protection de la vie privée de l'Ontario
2 rue Bloor Est, Bureau 1400
Toronto (Ontario) CANADA
M4W 1A8
Téléphone : 416-326-3333 • 1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca
This publication is also available in English.

papier recyclé à 30%

ISSN 1188-3006