Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 12
May 2007

Encrypting Personal Health Information on Mobile Devices

Section 12 (1) of the *Personal Health Information Protection Act, 2004* (*PHIPA*) sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

The Office of the Information & Privacy Commissioner/Ontario recognizes that the delivery of health care may require the use of PHI outside of the workplace, and that such PHI may most effectively be transported and used in electronic form. Notwithstanding the ease of use and portability of electronic documents, it is still important that only the minimum necessary data be transported in this manner.

Because of the high incidence of loss or theft of mobile devices such as laptop computers, personal digital assistants (PDAs), or flash drives, custodians need to ensure that personal health information that is stored on mobile devices is encrypted. When encryption is implemented properly, it renders PHI safe from disclosure. The availability of encryption means that it is easier to safeguard electronic records of PHI than it is to safeguard paper-based records when being transported.

This fact sheet is for health information custodians who store PHI on mobile devices. If you are unsure of the meaning of these guidelines, please consult a computer systems security expert to determine how to apply this fact sheet to the information in your care. In many cases, encryption can be as easy as installing a simple program and implementing proper key management for the system.

Why are login passwords not enough?

It is not acceptable to rely solely on login passwords to protect PHI on devices that are easily stolen or lost. 'Strong' login passwords will prevent casual access to data on a device, but may not prevent access by knowledgeable thieves. Strong login passwords are usually characterized by:

- No dictionary words;
- A combination of letters, numbers and symbols;
- 8 or more characters, with 14 or more being ideal.

For example, "**LetMeIn**" is a weak password because it uses dictionary words. On the other hand, you could remember the phrase, "My birthday is October 21 and I'm 25" which becomes the password "**MbiO21&i25**". This would qualify as

a strong password. Because strong passwords can be difficult to remember, however, users often create weak passwords. In addition, even strong login passwords may be written down, stolen, shared, hacked, or cracked with readily available software.

What is encryption?

Encryption is a process by which ordinary text or data, referred to as 'plaintext,' is turned into an unintelligible stream of seemingly random symbols, referred to as 'cyphertext.' This process is controlled by a digital 'key,' which will allow access to the encrypted data. The key could be:

- something you know, such as a 'strong' password distinct from a login password, since there are well known methods for cracking login passwords; or
- something you have, such as a USB drive or token; or
- something about you, such as your fingerprint scan or your signature.

Without the key, the data is unreadable. For example, the phrase "plain text" could be transformed to "~Sš£WÕN3@ƒ" when encrypted. The effectiveness of encryption depends on both the encryption standard and the strength of the key used.

Are there options?

Encryption can be implemented in a number of different ways on mobile devices.

Whole disk (drive) encryption

Sometimes referred to as whole disk encryption, this is a system in which an entire hard drive is encrypted. It is the preferred option for implementing encryption on new systems, and should be considered as a requirement for any new mobile device. Also, new system purchases may be the easiest way to implement encryption. Alternatively, whole disk encryption software is available from multiple companies. A web search for 'whole disk encryption' or discussions with a vendor will yield a number of possibilities for consideration. Typically, installation on individual laptops is no more difficult than installing any other software.

Whole disk encryption is potentially the most secure option available to health information custodians who feel they must store PHI on mobile devices.

Virtual disk encryption

A 'virtual' disk is a file that is created on an existing drive. The encryption software encrypts the entire file and treats it as if it were a new drive on the system. This typically requires the acquisition and installation of virtual disk or disk imaging software. Access to the encrypted virtual drive will typically require the use of a strong password, distinct from a login password. Without the password, and the encryption software, the virtual drive is undecipherable.

Virtual disks could be the only viable option on PDAs where the option of applying whole disk encryption may not be available. Virtual disks are also useful for older laptop computers. However, since many systems or software programs automatically create temporary files or backup files, virtual encryption is only effective if these unencrypted temporary or backup files are also either encrypted or deleted after use.

Folder or Directory encryption

Current operating systems provide some built-in encryption options. For example:

- If you have a Microsoft Windows XP™ system, you may be able to right click on a folder, and click on the 'Advanced' button that is visible under the 'General' tab. Select "Encrypt contents to secure data" to enable encryption.

- If you have an Apple OS X™ system you can encrypt your home folder by enabling "File Vault" from your System Preferences – Security Pane.

But while these options are easy to use, because they rely on the users' login password, they provide only limited protection and are insufficient, in and of themselves, for the safeguarding of PHI. They are vulnerable in that if a person gains access to the user's password, they will then have access to the data.

Device encryption

An alternative to storing PHI on a laptop is to store the data on a portable storage device, such as a USB key or 'thumb drive'. Portable music players and PDA's may also have this functionality. The portability of such devices is matched by the frequency with which they are lost, which further reinforces the need for encryption.

Like hard drives, there are options to encrypt the entire device or just the parts of the device that contain PHI. If you have acquired software to create a virtual disk, as described above, this same software may well have the capability of encrypting portable storage devices.

Enterprise encryption

This section is for health information custodians who are responsible for substantial numbers of devices, whether they be laptops, PDAs, or mobile storage. Relying on individual users to select and implement one of the encryption options described above may not be a viable option. There are enterprise-wide solutions that will enable custodians to enforce encryption standards on all devices under their control. A web search for, or a discussion with your vendor in the category of, "Data Leak Prevention" or "Information Loss Protection" or "End Point Protection" will reveal a number of options. Such tools may themselves do the encryption, or may work in conjunction with an already installed encryption tool and enforce enterprise policies.

In the context of a larger enterprise, the necessity for proper training, and the creation of a culture of privacy, cannot be minimized. Without significant executive support and staff acceptance, no encryption program will succeed.

Encryption standards

At the time of writing this fact sheet, the standard most recommended for secure storage of data was AES, or Advanced Encryption Standard. The strength of the version of AES selected depends on its key length. AES-128 is sufficient, but AES-192 or AES-256 are much stronger. Since encryption standards are always evolving, custodians are responsible for ensuring that any solution that is selected meets the generally accepted standards in effect, at the time. Encryption installations need to be regularly reviewed and updated, as necessary. If in doubt, please refer to a reputable security expert.

Off-site backup

Many companies back up their data to tapes or other media and store these media in locations outside of their data centres. Typically, these media are physically transported to off-site locations. Custodians should be aware of the

risk of the loss of these media and ensure that encryption or other methods are used to ensure that the information they have protected, in the event of a lost or stolen laptop, is not exposed through the loss of unencrypted data on their back up tapes.

Conclusion

The Commissioner has stated that in the event that a mobile device is lost or stolen, it will not be regarded as a privacy breach if sufficient safeguards were in place to ensure that PHI was not disclosed. Properly encrypted data would save custodians considerable time and money by allowing them to avoid the notification requirements of the *Act*, and prevent the potentially irreparable damage to a custodian's reputation resulting from the loss or theft of PHI. More importantly, it would protect individuals from the undue stress of knowing that their PHI had been lost or stolen.

Encryption checklist

- ✓ I have minimized the amount of PHI that I have on portable devices (preferably none in identifiable form).
- ✓ I delete PHI from all portable devices as soon as I have finished working with it.
- ✓ I know what PHI is stored on each of my portable devices.
- ✓ I have enabled my operating system encryption.
- ✓ I have purchased a system with whole disk encryption.

  OR
- ✓ I have purchased software to implement whole disk or virtual disk encryption on my laptop or PDA.
- ✓ If I use portable storage devices like USB keys, I buy them with encryption installed, or install encryption on them before I use them to store PHI.
- ✓ If I use a password to access encrypted data, it is a strong password AND it is different than the password that I use to login to my computer.
- ✓ I never write my password down.
- ✓ I do not share my password with anyone.
- ✓ If I don't use whole disk encryption, I can identify where ALL of the PHI on my system is stored.
- ✓ I only store PHI on the encrypted disk.
- ✓ I regularly verify or audit that my encryption policies are in fact being implemented and followed.

Solutions

The IPC recognizes that this encryption software may well be unfamiliar to those who have a responsibility for PHI data protection. The following are a sample of several encryption solutions currently available. This is neither an endorsement nor a recommendation, but we have tried to capture representative companies for the various types of solutions that are available. Please note that this type of technology changes rapidly and that what may be state of the art today. may not be, tomorrow.

Solution	Description	Website
CryptoMill	CryptoMill provides an enterprise end point security solution, including encryption in the SeaHawk product.	http://www.cryptomill.com
PGP	PGP provides a range of encryption solutions, including PGP Whole Disk Encryption.	http://www.pgp.com
TrueCrypt	An open source and freely available solution for virtual disk or whole disk encryption on Windows or Linux systems.	http://www.truecrypt.org
Vontu	Vontu provides enterprise data loss prevention solutions, including policy enforcement of encryption polices.	http://www.vontu.com
WinMagic	WinMagic provides a number of encryption solutions, including SecureDoc Hard Disk Encryption and SecureDoc Mobile Edition.	http://www.winmagic.com

Fact Sheet

is published by the **Office of the Information and Privacy Commissioner/Ontario**.

If you have any comments regarding this newsletter, wish to advise of a change of address, or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Cette publication, intitulée « Feuille-info », est également disponible en français.