

# STOP. THINK. PROTECT.

## Patient Privacy is in Your Hands.

As health care practitioners, many of you are accustomed to dealing with loss. You interact with people every day who have lost their health, lost a loved one, or perhaps simply lost hope. And you are experts at helping people work through and manage that sense of loss.

But what if you, yourself, were responsible for the loss of something that a patient may never get back: their privacy?

Earlier this year, a health care professional did something seemingly well-intentioned: she placed a USB key into her purse as she left the office, planning to do some work at home. As it happened, the files in question were the records of personal health information of 763 patients.

Her purse was stolen. And all the records – unencrypted and easily read by anyone – were lost. Lost, too, was the sense of privacy of those 763 patients.

Scenarios such as this have been played out countless times all across Ontario. Indeed, in recent years, the unencrypted health information of over 100,000 patients on laptops, USB keys and other mobile computing and storage devices has been lost or stolen. It's a privacy problem of epic proportions, compromising some of the most sensitive and personal types of information possible. And it must stop.

The *Personal Health Information Protection Act* requires that you take reasonable steps to ensure that personal health information is protected against theft, loss, and unauthorized use and disclosure.

Mobile devices, such as laptops, PDAs, and USB keys, add a new layer of complexity to this task. The great advantage of these devices – portability – is also their greatest vulnerability, making them easily susceptible to loss and theft.

For that reason, personally identifiable health information should not be stored on any mobile devices unless it is absolutely necessary. And when it is, you can – and **must** – take steps to minimize the risks to privacy.



## **STOP.**

Ask yourself: Do I really need to store any personal health information on this device?

## **THINK.**

Consider the alternatives. For example, would de-identified or coded information serve the same purpose? Can you access the information remotely through a secure connection or virtual private network instead?

## **PROTECT.**

If you must store personal health information on mobile devices it must be encrypted and protected with strong passwords. In addition, you must store the least amount of information possible, for the shortest amount of time.

For more information, access the following documents on the website of the Information and Privacy Commissioner of Ontario at [www.ipc.on.ca](http://www.ipc.on.ca).

- [Fact Sheet - Encrypting Personal Health Information on Mobile Devices](#)
- [Fact Sheet - Health-Care Requirement for Strong Encryption](#)
- [Safeguarding Privacy In a Mobile Workplace](#)

