Personal Health Information Protection Act, 2004

REPORT

FILE NO. HI-050012-1

A Community Care Access Centre

Personal Health Information Protection Act, 2004

REPORT

FILE NO. HI-050012-1

INVESTIGATOR: Nancy Ferguson

SUMMARY OF INFORMATION GIVING RISE TO THIS REVIEW:

A Community Care Access Centre (the CCAC) reported that 24 computers were missing following a break and enter. The matter was reported to the police and the Office of the Information and Privacy Commissioner/Ontario (the IPC). The CCAC undertook a consideration of its obligations under the *Personal Health Information Protection Act, 2004* (the *Act*) including the notification of the affected clients.

RESULTS OF THE REVIEW:

The CCAC wrote to the IPC to describe the loss, its investigation of the loss and the steps that would be taken to help prevent a similar incident from occurring in the future.

The CCAC reported that when staff arrived the morning following the break-in, they were asked to stay outside to permit police to conduct a thorough investigation and gather evidence. In some cases the cables locking the laptops to the work stations had been cut, in some cases the laptops were ripped away breaking the cable attachment.

The CCAC determined that the break-in occurred sometime before 11p.m. the previous evening, at which time a security alarm in the facility sounded.

The 24 missing laptop computers had been assigned to the CCAC's Case Managers, who visit clients to assess their needs and eligibility for services and monitor clients while they are receiving care. The Case Managers were using laptops computers as part of a province-wide program involving the standardized assessment of clients receiving home care. The Case

Managers use the laptops primarily to input data onto the standard assessment forms when they visit patients in their homes.

The CCAC advised that it obtained confirmation from its Manager of Information Systems about security policies and measures that were in place to protect patient personal health information (PHI). The CCAC provided the following information:

- the correct password had to be entered before the operating system would launch;
- an additional username and password, which was set to require a minimum of 12 characters, upper and lower case and mixed characters, must be entered to access the "active directories" on the local area network;
- all accounts are set to lock after three failed log-on attempts to the network and additional log-on attempts can only be made once an Administrator unlocks the account;
- staff were reminded to save documents containing PHI to the directories protected by encryption software (i.e., the standardized assessment tool used to gather client information during visits);
- staff were advised that PHI relating to patients gathered on the standardized assessment form during a visit, should be removed from the laptop when they were finished completing the assessment;
- each computer had a unique encryption key that was stored away from the laptops in a secure manner;
- staff were directed by default to save word processing documents to a file folder on the network and were advised not to save PHI to the hard drives of their computers.

The CCAC was of the view that it was highly improbable that PHI on the stolen computers would be accessible to unauthorized individuals, given the protections in place.

The CCAC advised that the active directory accounts of the missing laptops were disabled in the unlikely event that someone attempted to enter the office again and use a stolen laptop to try to gain access to the office network. All the Case Managers were asked to change their passwords following the incident.

The CCAC advised that the only way to determine exactly what had been saved on the laptop computers at the time of the loss was to ask the Case Managers and rely on their recollections.

The CCAC conducted interviews using an interview template and a spreadsheet to document the results. Case Managers were asked about the following issues:

- whether or not the Case Manager stored PHI on the local hard drive of their computer (e.g. the C:drive or the desktop);
- the level of security applied to PHI stored on the computer (i.e. use of passwords, where they stored documents containing PHI);
- the type of PHI on the computer;
- the names of clients whose PHI was stored on the computer;

- the Case Manager's view about the best method of communicating the loss of PHI to the affected clients.

The CCAC also checked to ensure that Case Managers had not written passwords in areas around their desks that would have been in plain sight during the break-in. The CCAC confirmed that education about this issue had been provided to staff in the past.

The Case Managers reported the following in terms of the PHI stored on their laptops:

- one Case Manager recalled that her laptop contained a document listing clients' names, addresses and information about diagnosis and treatment;
- three Case Managers recalled storing their clients' assessment tools on the laptop;
- one Case Manager recalled storing a letter to a client on a laptop.

The document containing the list of patient information had been "backed up" on the local network and could be reproduced in order to identify the affected patients. In the case of the assessment tools and the letter, the Case Managers could recall the clients' names.

Section 12(2) of the *Act* requires "Health Information Custodians" to notify patients if their PHI is stolen, lost or accessed by unauthorized persons. The CCAC sought input from the IPC on its notification plan. The CCAC indicated that its main concern was to provide notice in a manner that avoided creating unnecessary anxiety for its clients. Each affected client's situation was considered in order to determine how to most effectively carry out notification.

The CCAC notified each client who may have had PHI stored on a missing laptop. For the majority of the clients, the CCAC forwarded a letter indicating that the client's information had been stored on a laptop computer that was found missing following a break-in. The client was advised that the police and the IPC had been contacted and that there were security features in place on the laptop that the CCAC believed would protect the information. The CCAC invited any patient interested in obtaining further information to call their Privacy Officer. Case Managers were also prepared to respond to questions about the incident.

For some patients, it was determined that verbal notification was the most appropriate approach; for other patients, it was necessary to involve their substitute decision-makers.

Of the affected clients who contacted the Privacy Officer with questions or concerns, the majority related to concerns that the loss might expose them to identify theft.

The CCAC advised that, as a result of this loss and the resulting review, it has instituted the following security measures to help avoid a similar situation from occurring in the future:

- tested and verified the alarm system and its activation schedule;
- posted a security guard at its premises who performs routine security checks overnight;
- installed alarm system warning stickers on all entrances;
- installed additional sirens for the alarm;

- installed video surveillance devices on all entrance locations and drafted a policy on the use of this equipment using the IPC's "Guidelines for Using Video Surveillance in Public Places;"
- improved exterior locks and door handles;
- sent out reminders to all staff that PHI is not to be saved to computers unless absolutely necessary, such as during home visits;
- created a policy on safe laptop usage;
- monitored their systems log to check for any unusual activity.

Finally, the CCAC advised that while it had not notified the IPC immediately after this loss had occurred, in future it would do so, having further considered it and now having a better understanding of the IPC's role.

On the basis of all of the above, it was determined that further review of this matter was not warranted and the file was closed.

November 25, 2005

Ann Cavoukian, Ph. D.
Commissioner