

INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA

Report of an Investigation Concerning a Stolen Laptop Computer

December 5, 2006

Calgary Health Region

Investigation Report H2006-IR-002

(Investigation H1441)

I Introduction

- [1] On October 26, 2006 Calgary Health Region (“the custodian,” or CHR) notified the Office of the Information and Privacy Commissioner of a potential breach of privacy involving a stolen laptop computer.
- [2] The Commissioner authorized me to conduct an investigation under section 84(a) of the *Health Information Act* (HIA). Section 84(a) allows the Commissioner to conduct investigations to ensure compliance with any provision of the HIA. This report outlines findings and recommendations resulting from my investigation.

II Background

- [3] A mental health therapist (“the affiliate”) employed by Calgary Health Region’s Collaborative Mental Health Program (“the Program”) reported the theft of a laptop computer. This computer was issued to her by CHR. The affiliate had taken the laptop computer home to work on a presentation. She left her home for a few hours in the afternoon of Sunday October 21. The computer was turned off and placed on a desk. The house was locked. When she returned later that day, she discovered that the laptop had been stolen, along with a number of other articles from her home.
- [4] The affiliate immediately reported the theft to the Calgary Police Service and her employer. To date, the laptop computer has not been recovered.
- [5] A database of 1094 patient records from the Collaborative Mental Health Program was stored on the stolen computer. This database comprises the following information regarding the treatment and care of current and past patients – all children, under 6 years old:
 - a. Patient name, date of birth and personal health number (PHN)
 - b. Parent(s) name(s)

- c. Patient and parent address and telephone number
- d. Notes related to patients, such as patient history, family history, progress notes, developmental concerns, interactions with other professionals and summary of consultations.

In some cases, the database did not contain all of the above elements relative to each patient. At times, the patient's PHN was not included. Also, the parent address was not always included.

- [6] Some other records, similar to those above, may have been stored on the laptop computer outside of the database. These were contact notes on 14 patients held in relation to the affiliate's previous assignment with CHR's Community Child Mental Health Program at the South Calgary Health Centre. The affiliate is not certain whether these files were stored on the laptop at the time of the theft or had been deleted previously. All findings and recommendations presented in this Report apply to these records as well.
- [7] Members of the Program team are each issued a laptop computer to assist them in completing their work while away from the office. In fact, most work is done in the field, rather than at the Program's headquarters. When in the office, each team member downloads a copy of the entire Program database onto their laptop computer. While in the field, team members input various notes as described above. When they next return to the office, they upload any new data to the master database and download a new, up to date version of the master database.
- [8] According to the Program's brochure, Collaborative Mental Health Care is:

A community-based program to improve the conditions for young children's mental health through a variety of strategies, including consultation, education, advocacy and brief intervention in partnership with children's care providers.

The program is intended for children under 6 and delivered by a team of psychologists, social workers, nurses and child psychiatrists. Besides providing consultation, assessment, intervention and referrals, the program has an education component in which presentations and workshops are provided to child care professionals on children's mental health topics.

III Application of HIA

- [9] The *Health Information Act* applies to health information in the custody or control of custodians. Calgary Health Region is a regional health authority established under the *Regional Health Authorities Act* and consequently falls within the HIA definition of "custodian" under section 1(1)(f)(iv).

- [10] The mental health therapist is an employee of the Calgary Health Region. As an individual employed by the custodian, she is an “affiliate” as defined in section 1(1)(a)(i) of the HIA.
- [11] I have reviewed the database subject to this investigation and found it contains individually identifying registration information and diagnostic, treatment and care information, which is considered “health information” as defined in section 1(1)(k) of the HIA.
- [12] Under section 58(1) of the HIA, custodians have a duty to collect, use and disclose health information in a limited manner. That is, they must collect, use or disclose the minimum amount of health information needed to carry out an intended business purpose.
- [13] Under section 60 of the HIA, custodians have a duty to maintain administrative, technical and physical safeguards to protect the confidentiality of health information and the privacy of individuals. This section places particular emphasis on addressing the risks associated with electronic health records.

IV Issues

- [14] Did the custodian collect, use or disclose health information in contravention of section 58(1) of the *Health Information Act*?
- [15] Did the custodian fail to safeguard health information in contravention of section 60 of the *Health Information Act*?

V Findings

- [16] During the course of my investigation, I interviewed the affiliate whose laptop was stolen, the Program manager and CHR’s Director of Information Technology (IT) Security. I viewed a copy of the database and inspected a laptop computer with the same configuration as the one that was stolen. I also reviewed the facts of the theft and the custodian’s follow-up actions with the CHR Manager of Information and Privacy.

Using health information in a limited manner

- [17] Section 58(1) of the HIA states:

58(1) When collecting, using or disclosing health information, a custodian must [...] collect, use or disclose only the amount of health information that is essential to enable the custodian [...] to carry out the intended purpose.

- [18] As stated earlier, Program workers transfer a copy of the entire patient database onto their laptop computers when they work in the field. This database includes current and past patients. Most of the time, workers only need to view and update health information related to their current clients to support the objectives of the Program. CHR stated that the Program's therapists often help each other on cases and may have a business need to view records other than their own. Also, CHR pointed out that children in the Program are often referred multiple times from different sources. In such cases, the therapists would need to look at the old case file to get a sense of the child's history. Given these factors, I recognize the challenge CHR faced in implementing effective technical and administrative controls to meet its duty under section 58(1). However, the therapists' need to view files other than those associated with their current caseload is the exception, rather than the rule. There is no general need to view the entire database while in the field.
- [19] The more health information a worker brings outside of a secure office area, the greater the risk. Had the affiliate been able to copy information related only to her current caseload, this theft would have affected far fewer than 1094 families.
- [20] The database was set up in such a way that it was not possible to download only the information that was needed. The practice of downloading the entire database was established by the Program rather than the affiliate.
- [21] In establishing a business process where the entire database was downloaded by workers, I find that the custodian failed to meet its duty to use health information in a limited manner, contravening HIA section 58(1).

Duty to protect health information

- [22] I have divided my analysis of whether CHR met its duties set out in HIA section 60 into two parts. First, I focused on whether CHR adequately identified the risks associated with using laptop computers. Without an analysis of risk, it is difficult for any organization to implement appropriate safeguards. My intent was to demonstrate that a risk analysis would likely have mitigated the damage caused by this incident. Secondly, I examined the safeguards that were in place and analyze their effectiveness.
- [23] The relevant parts of section 60 of the HIA read as follows:
- 60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will
- (c) protect against any reasonably anticipated
- (i) threat or hazard to the security or integrity of the health information or of loss of the health information, or
- (ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,

- (2) The safeguards to be maintained under subsection (1) must include appropriate measures
- (a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records
- [24] Section 8 of the *Health Information Regulation* flows from HIA section 60 above. The relevant parts of the regulation state:
- 8(1)** A custodian must identify, and maintain a written record of, all of its administrative, technical and physical safeguards in respect of health information.
- (3)** A custodian must periodically assess its administrative, technical and physical safeguards in respect of
- (b) any reasonably anticipated threat or hazard to the security or integrity of the health information or to the loss of the health information, and
- (6)** A custodian must ensure that its affiliates are aware of and adhere to all of the custodian's administrative, technical and physical safeguards in respect of health information.

Protecting against reasonably anticipated threats

- [25] An important feature of section 60 is the duty of custodians to protect against reasonably anticipated threats to the security of health information. In order for a custodian to reasonably anticipate a threat, it follows that the custodian must perform a risk assessment to determine what possible threats may affect its health information and, in particular, information held in electronic form. Further, section 8(3)(b) of the *Regulation* above states that custodians must periodically assess their safeguards, which supports the notion of regular risk assessment.
- [26] The requirement to perform some form of risk assessment is a feature found in all information security best practice guidelines and standards. For example, the ISO 17799 Code of Practice for Information Security Management describes risk assessment in its introduction¹:

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

¹ International Organization for Standardization, Geneva, Code of practice for information security management, Reference number ISO/IEC 17799:2005(E), page ix.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results.

More specifically, section 11.7 of the Code states²,

When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protections applied.

Calgary Health Region uses the ISO 17799 Code of Practice as the basis for its information technology security policies.

- [27] The Program was initially a joint program between the Alberta Mental Health Board (AMHB) and CHR. AMHB funded the Program and CHR provided management and staffing. In 2003 the Program's funding was also transferred to CHR, giving the region full administrative responsibility. I saw evidence that CHR currently performs risk assessments for major deployments of mobile technology in other business areas; however, no assessment was performed for the Collaborative Mental Health Program. In this case, it appears that neither the Program's management nor CHR IT Services had considered the risks associated with the business practice of transferring the Program database onto laptop computers.
- [28] Section 64 says that PIAs must be prepared and submitted to our Office for comment before a custodian implements proposed administrative practices or information systems that involve collection, use or disclosure of individually identifying health information. Organizational change, as described above, could be interpreted to fall within the definition of "proposed administrative practices." Conducting a PIA would almost certainly have identified the risks of storing an unencrypted copy of the entire database on laptop computers. These risks could, in turn, have been mitigated. Whether the formal PIA requirement was triggered in this case is perhaps debatable. However, I have already shown that a risk assessment of some kind was required under the HIA – a PIA would have fulfilled this obligation.
- [29] I will cover CHR's overall response to the incident in more detail later, but I highlight one point here. To prevent this kind of incident in the future, CHR is providing Virtual Private Network (VPN) technology to the Program. Properly configured, a VPN allows employees to access an organization's applications and data securely over the internet, eliminating the need to store data on mobile devices, such as laptop computers. This technology has been in use by other mobile workers at CHR for some time and is typically set up so that no data is copied to the remote computer. If CHR had conducted a risk assessment of the Program's business practices, it likely would have identified a need to implement VPN technology. Had the affiliate been using a VPN to access the Program database rather than storing it on her laptop, little or no health information would have been lost in the theft.
- [30] Risk assessments and PIAs can identify vulnerabilities that were previously unknown. This incident points to the benefit of conducting risk assessments of new and

² Ibid, page 74.

existing business practices on a regular basis. As can be seen from this case, risk assessments are particularly useful during periods of organizational change.

Analysis of safeguards

- [31] I have established the custodian's duty to perform a risk assessment when deploying mobile technology, such as laptop computers. While no formal risk analysis was done specific to the Collaborative Mental Health Program, some security measures were implemented as part of CHR's regular security practice. The main question in this part of my analysis will be to determine whether these measures were reasonable in light of the risks associated with mobile computing.
- [32] The risk of laptop computer theft is known to be high. This risk was well established by our Office in Investigation Report P2006-IR-005. In paragraph 64 of this Report, my colleague says, "Frequent incidents of laptop theft from employees, often despite corporate policies, are well known and publicized, making the risk real and foreseeable."
- [33] CHR has established a number of technical and administrative controls relative to laptop computers. These controls include policies, physical security controls and technology controls.
- [34] CHR has a policy named, "Laptop Security Practices," dated August 15, 2006, which provides guidance to affiliates on secure mobile computing. It covers laptop use when in a building and when traveling, data protection and reporting laptop thefts. The relevant points in this policy are listed below:

Physical Protection

A. In Building

- Use a locking cable or clamp to secure your laptop to a desk or table.
- Never leave your laptop unattended, particularly overnight on desktops. Lock it in a desk drawer or cupboard.

Data Protection

You should:

- Keep the amount of data stored on your laptop to a minimum.
- If you have to store sensitive information on the laptop, use data encryption tools to protect the information.
- Always use the secure operating system that is approved by the Calgary Health Region's ITS department

- [35] Further, the Mental Health Information and Evaluation Unit, which administers the Collaborative Mental Health Program, provided the following recommendations (among others) in a memo to all regional mental health employees, dated July 25, 2006:
- Always password protect your computer
 - Safe passwords are typically a minimum of 8 characters and use both upper and lower case letters, numbers and symbols
 - Always secure laptops and projectors using the cables provided while in use during the day.

- Always encrypt confidential information that you have stored on your laptop.
 - Please refer to [external company's website] for CHR recommended encryption software or contact Information Technology.
- [36] CHR's security policies in relation to laptop computers are sound. They are based on industry best practices, including the ISO 17799 Code of Practice, are up to date and reviewed regularly. The policies are an example of "defense in depth" where many different kinds of controls are applied in combination to mitigate the risk of theft or loss. I will now examine how these policies were implemented and whether they mitigated any potential harm caused by the theft.
- [37] The amount of data stored on the laptop was not kept to a minimum. As was discussed previously, there was no general need to download the entire database onto laptop computers. Program team members could have carried out their duties with data relating to their current caseload, plus some other data, as necessary (see paragraph 18). Clearly, had this measure been implemented, the number of individuals affected would have been much lower.
- [38] The affiliate's laptop computer was equipped with a locking cable. However, this cable was not used at the time of the theft. Employees naturally feel more secure at home and may not think to apply additional security controls. Further, CHR's policy is not explicit on this point. The affiliate also explained she didn't have anything to secure the cable to at home. Further guidance and training is needed on physical security. For example, CHR could make it explicit that the policy applies to home use and provide tips to employees on alternate ways to secure a laptop when no cable attachment point is available.
- [39] The laptop was running the region's recommended computer operating system, which included a log-on feature. The user needs to enter a user name, followed by a password. The password met CHR's strong password standard. All CHR laptop computers have this standard configuration. Using an operating system log-on and password is good practice and will deter casual attempts to access the computer. However, these passwords are not foolproof and can be by-passed by someone with sufficient skill and motivation. Many password cracking tools are readily available for free on the internet (for example, see the entry at Wikipedia.org for "password cracking").
- [40] The database containing patient information was protected by two passwords, one to open the database interface and another to access the data. These two passwords did not meet CHR's strong password standard. In any case, their usefulness is questionable as such passwords are easily cracked or bypassed. Assuming an attacker is capable of getting past the operating system password, the database passwords offer little additional protection.
- [41] Encryption (i.e. applying cryptographic controls) is a way to scramble data to make it unreadable. Only those who have the encryption key can decode the scrambled data. The custodian's policy on encryption was not implemented. This is unfortunate. Had sufficient cryptographic controls been properly applied, the data would have

been virtually inaccessible and the risk to affected individuals negligible. Rather than systematically implementing encryption in areas of high risk, CHR's policy points users to a website that offers free encryption software for download. In my view, it is not reasonable to count on non-technical employees to determine whether they need encryption software, download it, configure it and use it properly. For a large organization such as CHR, cryptographic controls should be implemented at the enterprise level based on a risk analysis and should be centrally managed and supported.

- [42] In addition to the above controls specifically related to laptop computers, CHR provides general privacy and security awareness training. The affiliate completed this training and also signed a confidentiality agreement stating that she would follow the custodian's privacy and security policies. Awareness training is good practice and required by the HIA; however, based on my observations above, I do not believe the custodian provided the affiliate with sufficient guidance and direction to mitigate the specific risks of using a laptop computer.
- [43] While the custodian's policies reflect a "defense in depth" strategy, their implementation does not. Of the relevant laptop security controls listed in policy, only the password control was implemented and followed. Again, referring to P2006-IR-005, our Investigator said in her conclusion, "A log-on password is not sufficient to satisfy the requirement for reasonable safeguards." In this case, the custodian clearly intended to provide more protection than a log-on password, but the execution of the policy fell short. If the security measures outlined in policy had been implemented, I would likely have concluded that they were reasonable, but in this case I cannot.
- [44] The custodian failed to conduct a risk assessment to determine the most appropriate safeguards to implement. Further, it did not assess whether CHR security policies were in fact implemented. Finally, the custodian did not adequately train its affiliates in how to use laptop computers securely. Therefore, I find the custodian did not meet its duty to protect health information, in contravention of section 60 of the *Health Information Act*.

VI Assessment of risk caused by theft

- [45] CHR conducted a thorough analysis of privacy risk to patients caused by this theft, which I reviewed. It concluded there is a low risk that the health information would be accessed, but that it would be in patients' best interest to notify them of the possibility.
- [46] I performed my own assessment of risk to the individuals whose health information was stored on the stolen computer. In doing so I considered three factors: the likelihood the data can be accessed, the nature of the information and the harm that may be caused by its disclosure.

- [47] As discussed earlier, the only security measure protecting the stolen laptop is a series of passwords. Password protection can be cracked by a motivated and knowledgeable attacker. It is not known whether the thief in this case has these skills, nor is it known whether the thief gave or sold the computer to someone who could exploit its security vulnerabilities. It is equally likely the computer's data was completely erased and the laptop is being used by someone who will never know it contained sensitive health information. Unfortunately, there is no guarantee of this being the case. Had the data been properly encrypted, I could conclude that there would be little or no risk. In this case, I must conclude that there remains a possibility that the health information could be accessed.
- [48] The information in the database does not give an identity thief everything he needs to engage in fraud. However, it does contain names, addresses, dates of birth, and personal health numbers. This information, used in combination with other information and fraud techniques, can be a starting point for identity theft. This risk is somewhat mitigated by the fact that most of the entries in the database were for children under 6 years old, who likely do not have any credit history (although some parents' information was also included). Therefore, the likelihood of identity theft is relatively low, but cannot be dismissed entirely.
- [49] Despite the low risk of identity theft, it must be said that the information on the stolen laptop is highly sensitive. It consists of children's mental health history and diagnoses. In some cases, the data touch on family members as well. The affected individuals would clearly be very upset if this health information fell into the wrong hands.
- [50] In a case such as this, where risk cannot be ruled out and the information is very sensitive, it is appropriate for the custodian to notify the affected individuals to advise them of the possible privacy risks (see H2005-IR-001). This is standard practice at CHR and the notification process is now complete.

VII Actions taken by the custodian

Notification

- [51] On November 9, CHR issued a news release about the stolen laptop, describing the information that was lost and informing the public of the actions taken so far. CHR also committed to notifying those patients directly affected by the theft.
- [52] On November 16, CHR contacted current patients by telephone to provide notice. Past patients were notified by mail between November 20 and 30. In both cases, patients were given an overview of the health information that was lost and CHR's assessment of risk to their privacy. Patients received information on how to contact credit monitoring agencies in case they were concerned about identity theft. Finally, CHR informed affected individuals that they could contact our Office if they had further concerns about the incident.

- [53] The 14 patients whose records may have been on the laptop (see paragraph 6) were also informed using the above protocol. As stated earlier, CHR is unable to confirm whether these records were stored on the laptop at the time of the theft. CHR has contacted these individuals as a precautionary measure.
- [54] In my view, these measures constitute adequate notice.

Security improvements

- [55] Only weeks before the theft, CHR's IT department received budget approval to implement an enterprise-wide encryption solution for mobile computing. Based on a risk analysis, CHR has prioritized installation of the encryption software in business areas where laptops containing health information and other sensitive data are in use. This project is now underway and it is expected that the solution will be fully implemented by mid-January 2007. CHR's mental health area, which includes the Collaborative Mental Health Program, is included on this priority list.
- [56] CHR will also be equipping high-risk laptop computers with "phone-home" technology. If a laptop computer equipped with this system is stolen, the first time it is connected to the internet, it sends a signal back to CHR. At this point, CHR would have the option of tracking the computer's location, if possible, or of sending a signal back to the computer that destroys its hard-drive data.
- [57] Until the encryption solution is available, Program staff will be using Virtual Private Network (VPN) technology to access the database remotely. The VPN will allow workers to access the database from their laptops over an encrypted internet connection. The advantage of this method is that it allows workers to use the master database without having to store any health information on their laptop computers. If a laptop is stolen, it will contain no health information from the Program database. The VPN will be accessed through a strong authentication mechanism making it unlikely that the VPN could be compromised if another laptop is stolen.
- [58] The Program database cannot be re-configured to give workers access to their current patients only. It is expected that the database will be retired approximately two years from now and replaced with another system that has appropriate need-to-know controls in line with the custodian's HIA duty to use health information in a limited manner. In the meantime, this duty will be re-enforced through policy and education.
- [59] CHR has securely deleted copies of the database from the rest of the laptop computers used by Program staff.

VIII Recommendations

- [60] I made a number of recommendations to CHR, which they agreed to follow:
- a. Review need-to-know policies to ensure that affiliates are only using the amount of data they need to carry out their duties.
 - b. Review policy on mobile computing to ensure it addresses the associated risks.
 - c. Perform a review of mobile computing deployment to find any other business areas where identifiable health information is stored unencrypted on mobile devices. Mitigate any identified risks with appropriate safeguards.
 - d. Prior to deploying mobile computing devices, conduct a risk assessment or Privacy Impact Assessment to determine appropriate safeguards.
 - e. Provide specific training to affiliates who have been issued mobile computing devices. This training should make affiliates aware of the risks associated with mobile computing, as well as provide detailed instructions on how to secure these devices.

IX Conclusion

- [61] Custodians have a duty to write polices to facilitate implementation of the *Health Information Act*. Calgary Health Region wrote sound privacy and security policies. Unfortunately these polices were not effectively implemented and CHR was found in contravention of the HIA. I am satisfied with the actions CHR took to notify patients of this incident and the commitments they made to mitigate similar problems in the future. CHR acted quickly to address this theft and worked cooperatively with our Office throughout this investigation.
- [62] Mobile computing technology is widely deployed in Alberta's health sector. Other custodians would do well to learn from this incident. Our Office makes the following general recommendations regarding mobile computing:
- Perform a Privacy Impact Assessment (which should include an assessment of security risks) before implementing mobile computing.
 - Do not store personal or health information on mobile computing devices unless you need to – consider technologies that allow secure, remote access to your network and data instead.
 - If you must store personal or health information on a mobile device, use encryption to protect the data – password protection alone is not sufficient.
 - Keep the amount of personal or health information stored on mobile computing devices to a minimum, based on your business needs.
 - Periodically check your policies against practice to ensure they reflect reality and remain effective.
 - Provide specific training on mobile computing to staff to ensure they understand the risks and understand how to protect their equipment.

Brian Hamilton, CISA
Portfolio Officer, Health Information Act
Office of the Information and Privacy Commissioner of Alberta