

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

Report on the Investigation into Stolen Computers Containing Health Information

from

HealthWise HomeCare Inc.

August 16, 2002

Investigation Report # H0054 & H0056

I. Introduction

[para 1] On March 6, 2002 the Information and Privacy Commissioner (Commissioner) received a report from the Capital Health Authority (CHA) that computers containing individually identifying health information had been stolen from their affiliate, HealthWise HomeCare Inc. (the Affiliate). Aspen Regional Health Authority # 11 (Aspen) reported this incident to the Commissioner, as HealthWise HomeCare Inc. is also their affiliate.

[para 2] The Commissioner ordered an investigation into this matter under section 84(a) of the *Health Information Act* (HIA). This report outlines the findings and recommendations of this Office.

II. Background

[para 3] Alberta's HIA came into force on April 25, 2001. This law applies to custodians, which includes regional health authorities and other health service providers paid by the Alberta Health Care Insurance Plan to provide health services. The law also applies to an affiliate of a custodian. The HIA defines an affiliate as an individual employed by a custodian, a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian. CHA and Aspen both have contracts with the Affiliate to provide home care services to their clients. As such, the HIA applies to CHA, Aspen and the Affiliate.

[para 4] On the weekend of February 15 to 18, 2002 the Affiliate's office was broken into and two computers were stolen. The computers contained the following information about CHA and Aspen clients:

Patient's first and last name, birth date, address, phone number, affiliate identification number, contact person, physician name, reason for referral, health history, client sensitivities, health concerns, medications, treatment, community agencies involved, caregiver level assigned, and general notes and comments.

[para 5] Under section 1(1)(k) of the HIA, ‘health information’ means any or all of the following:

- (i) *diagnostic, treatment and care information;*
- (ii) *health services provider information;*
- (iii) *registration information.*

[para 6] Therefore, I find that the information contained in the computers is ‘health information’.

III. Investigation Findings

[para 7] The following issues are examined in this report:

1. Did the Affiliate have reasonable physical security measures in place to protect health information?
2. Did Capital Health Authority take reasonable steps to maintain administrative safeguards to protect health information?
3. Did Aspen Regional Health Authority # 11 take reasonable steps to maintain administrative safeguards to protect health information?

Issue 1: Did the Affiliate have reasonable physical security measures in place to protect health information?

[para 8] The relevant portion of the HIA states:

62(1) Each custodian must identify its affiliates who are responsible for ensuring that this Act, the regulations and the policies and procedures established or adopted under section 63 are complied with.

62(4) Each affiliate of a custodian must comply with

(a) this Act and the regulations, and

(b) the policies and procedures established or adopted under section 63.

63(1) Each custodian must establish or adopt policies and procedures that will facilitate the implementation of this Act and the regulations.

[para 9] Section 62(4) requires an affiliate of a custodian to comply with the HIA, regulations and the policies and procedures established or adopted by the custodian under section 63. As such, I have examined the physical safeguards that the Affiliate had in place at the time of this incident.

[para 10] The standard required by the HIA for physical security is reasonableness. The relevant portion of section 60(1) says:

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 ...

[para 11] In Order 98-002 the Commissioner accepted the definition of ‘reasonable’ in Black’s Law Dictionary which reads:

Fair, proper, just, moderate, suitable under the circumstances. Fit and appropriate to the end in view ... Not immoderate or excessive, being synonymous with rational, honest, equitable, fair, suitable, moderate, tolerable.

[para 12] In my view, determining reasonable measures to protect health information can only occur following a custodian and or affiliate’s assessment of risk based on all known relevant circumstances. Reasonable measures would be those that are suitable under the circumstances.

[para 13] I have attended the Affiliate’s business site to examine physical security arrangements. While I will not comment on specific security arrangements, the Affiliate did have locks on exterior doors, paper files in locking cabinets, computers password protected and a monitored security system. Taking this into account, as well as other information provided to me by the Affiliate, I find that they had taken reasonable measures to physically secure health information.

[para 14] In hindsight, the Affiliate could have taken additional measures to protect health information. The Affiliate has recognized this and has since upgraded their on-site security.

Issue 2: Did Capital Health Authority take reasonable steps to maintain administrative safeguards to protect health information?

[para 15] As previously noted, the HIA requires that custodians establish or adopt policies and procedures to facilitate implementation of the Act. Although I found that the Affiliate had taken reasonable measures to protect health information, I must also examine whether or not CHA met their obligations in this matter. In other words, did the CHA provide the Affiliate with policies and procedures that would facilitate ensuring that health information had been properly protected?

[para 16] The relevant sections of the HIA state:

60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will

(a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,

(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, and

(d) otherwise ensure compliance with this Act by the custodian and its affiliates.

62(1) Each custodian must identify its affiliates who are responsible for ensuring that this Act, the regulations and the policies and procedures established or adopted under section 63 are complied with.

63(1) Each custodian must establish or adopt policies and procedures that will facilitate the implementation of this Act and the regulations.

Regulation 8(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.

[para 17] The HIA requires a custodian to establish or adopt policies and procedures to facilitate implementation of the Act and to maintain administrative, technical and physical safeguards. This investigation examines whether or not administrative safeguards have been maintained. In my view, to satisfy the HIA requirement to maintain administrative safeguards a custodian must have policies and procedures related to both the protection of confidentiality (section 60(1)(a)) and security (section 60(1)(c)) of health information.

[para 18] What I must examine is whether the custodian has adequately maintained administrative safeguards that 1) protect confidentiality of health information and 2) protect against any reasonably anticipated threat to the security of health information.

A. Were administrative safeguards maintained to protect confidentiality of health information?

[para 19] CHA said that on December 28, 2001 the CHA "Health Information Directive" and procedures (Health Information Directive) were provided to the Affiliate in compliance with the HIA.

[para 20] I have reviewed the Health Information Directive and found that it contains corporate policies and procedures concerning collection, use and disclosure of health information. As such, I find that the Health Information Directive is an administrative safeguard designed to protect confidentiality of health information and serves as corporate policies and procedures that facilitate implementation of the Act. Further, by communicating these policies and procedures and holding regular Capital Health Home Care Contracted Agency meetings where HIA issues may be addressed, I find that CHA has reasonably complied with the requirement to ensure compliance of the Affiliate.

[para 21] Accordingly, I find that CHA has complied with the requirement under section 60(1)(a), 63(1) and regulation 8(6) to maintain administrative safeguards to protect the confidentiality of health information and to take reasonable steps to ensure that the Affiliate is aware of and adhering to these safeguards.

B. Were administrative safeguards maintained to protect against any reasonably anticipated threat to the security of health information?

[para 22] My review of the Health Information Directive found that it relates only to the protection of confidentiality of health information. It does not include administrative safeguards to protect against any reasonably anticipated threat to the security of health information.

[para 23] CHA provided me with a draft copy of the “Health Information Security Directive” and procedures (Health Information Security Directive). At the time that the computers were stolen this Health Information Security Directive had not been approved nor had it been provided to the Affiliate. While the Health Information Directive refers to the requirement for appropriate security systems and procedures, this is stated in the context of collection, use and disclosure of health information, not health information security. The Health Information Directive appears to recognize this, as it states that CHA will “introduce policies and procedures that protect against any threats or hazards to the security or integrity of the information or loss of the information.”

[para 24] CHA also advised that the CHA Homecare policy, specific to homecare affiliates, states that “Homecare staff will ensure that client records are stored safely and securely (on site or off site) and that the information is handled confidentially.” While CHA has generally advised the Affiliate that they must protect health information by ensuring that they have appropriate security systems, I do not see this as meeting the HIA requirement to maintain safeguards, including the establishment or adoption of policies and procedures.

[para 25] At the time of the theft CHA had not established or adopted corporate policies or procedures to protect against threats or hazards to the security or integrity of health information. As such, CHA has not sufficiently maintained administrative safeguards for the security of health information.

[para 26] Accordingly, I find that CHA is not in compliance with the requirement under section 60(1)(c) and 63(1) of the HIA. It follows that CHA is also not in compliance with the requirement under regulation 8(6) to ensure that the Affiliate is aware of and adhering to these administrative safeguards.

[para 27] However, there is no information before me that would lead me to believe that even should CHA have fully met their requirements to maintain administrative safeguards that this would have prevented the theft. CHA has expended resources to develop comprehensive privacy policies and procedures and their efforts in this regard should not be overlooked. Prior to the release of this report, CHA advised me that the Health Information Security Directive has now been approved and CHA has since provided it to all of its affiliates.

[para 28] In addition, CHA has taken a very proactive and positive approach in addressing this incident. CHA, upon being notified of the breach by the Affiliate, immediately initiated an internal review, reported to the Commissioner, and began to address any potential security gaps with this and other CHA affiliates.

Issue 3: Did Aspen Regional Health Authority # 11 take reasonable steps to maintain safeguards to protect health information?

Were administrative safeguards maintained to protect confidentiality of health information and to protect against any reasonably anticipated threat to the security of health information?

[para 29] During my investigation, Aspen advised me that they have not established or adopted policies and procedures to facilitate implementation of the HIA. This position was the result of a policy decision that new policies and procedures would not be created for those matters detailed in the HIA or the regulations. Aspen stated that they did not feel that it was necessary to develop policies and procedures that mirror legislation.

[para 30] Maintaining safeguards and developing policies and procedures to protect health information is not discretionary. The language of section 60 and 63, ‘must take reasonable steps ... to maintain safeguards’ and ‘must establish or adopt policies and procedures’, make these provisions mandatory.

[para 31] I find that Aspen has not maintained administrative safeguards to protect the confidentiality of health information, nor to protect against any reasonably anticipated threat to the security of health information, including establishing or adopting policies and procedures.

[para 32] Accordingly, I find that Aspen has not complied with the requirements under sections 60(1)(a)&(c) and 63(1).

[para 33] It follows that Aspen is also not in compliance with the requirement under regulation 8(6) to ensure that the Affiliate is aware of and adhering to these administrative safeguards.

[para 34] As was the case with CHA, there is no information before me that would lead me to believe that even should Aspen have met their requirements to maintain administrative safeguards that this would have prevented the theft.

[para 35] In hindsight, Aspen has said that it recognizes the obligation to develop written policies. In addition, Aspen has completed a risk assessment of this theft and revised some of its internal practices that will assist them in ensuring that their affiliates comply with the HIA.

Closing Comment

[para 36] I have found that the Affiliate had taken reasonable steps to protect health information.

[para 37] I also found that CHA partly complied with sections 60(1), 63(1) and regulation 8(6) of the HIA. To fully comply, CHA must complete and provide to the Affiliate the Health Information Security Directive and take steps to ensure that the Affiliate complies with this Directive. As previously noted, CHA has already completed this task. Accordingly, I am not making any recommendations to CHA in this report.

[para 38] I commend the CHA and the Affiliate for their co-operation in this investigation and the diligence of their staff in addressing this matter.

[para 39] With respect to Aspen, I found that they have not complied with sections 60(1), 63(1) and regulation 8(6) of the HIA. I have discussed this matter with Aspen who have agreed to provide the Commissioner with an implementation plan within 30 days of the release of this report that establishes a time line for the approval of administrative safeguards to be communicated to their affiliates and addresses Aspen's plan to ensure compliance.

Submitted by

LeRoy Brower
Health Team Leader