

INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA

Investigation Report Concerning Stolen Laptops Containing Health Information

November 5, 2007

Capital Health

Investigation Report H2007-IR-002

(Investigations H1652, H1726, H1733, H1742 & H1746)

I Introduction

[1] On May 25, 2007, the Information and Privacy Commissioner received a privacy breach report from Capital Health that four laptops containing health information had been stolen from a Capital Health office.

[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 investigate to ensure compliance with any provision of the Act. This report outlines findings and recommendations resulting from my investigation.

II Background

[3] On May 8, 2007, four laptops were stolen from a Capital Health office. Capital Health reported the theft to the police on May 9th.

[4] On June 12, 2007, the Commissioner received an investigation report from Capital Health. The report said the laptops were used by Information Systems application coordinators and system analysts who provide computer systems support to clinical program areas. The laptops contained health information obtained while providing this support, and some information about the individuals to whom the laptops were assigned. The laptops were protected with power-on and administrator passwords.

[5] Capital Health met with our Office on June 13, 2007, where it was agreed that additional risk assessment and consideration to provide notice to affected individuals was required. An informed decision about notification cannot be made before risk to affected individuals has been fully assessed. Such an assessment must consider:

1. The level of risk that the information can be accessed, and

2. If accessed, the level of risk due to the sensitivity of the information or ability to cause harm by using the information

[6] Capital Health agreed to complete a risk assessment on this basis and on July 13, 2007, advised me it believed the risk of unauthorized access to health information was low, but due to the nature of the information, decided to provide notice to all affected individuals.

[7] On August 1, 2007, Capital Health began notifying individuals by mail. On August 2nd Capital Health issued a news release to notify the public about the incident.¹

III Notification to Affected Individuals

[8] The purpose of notice is to afford affected individuals an opportunity to mitigate harm that could occur as a result of a breach. Some notified individuals expressed concern to our Office that it took Capital Health nearly three months from the time of the theft to the time they were notified.

[9] Capital Health determined they needed to notify more than 20,000 affected individuals in response to this incident, which created logistical and resourcing issues that delayed the notification process. Time was required to accurately reconstruct the information that was held on the laptops and develop a list of individuals to notify. In addition, addresses needed to be verified to ensure notice letters were not mailed to the wrong location or to any deceased individuals.

[10] When a breach occurs, notice should be provided as quickly as possible, but speed should not replace a due diligence assessment of the manner and method of notice that ensures affected individuals are provided with accurate and useful information. A prompt notice provides opportunity for an individual to take protective action before harm occurs, or minimize or stop harm that has already occurred.

[11] In this incident, I am mindful that notice was being provided as a preventative measure. There was no evidence the information on the laptops had been accessed or was being used to cause harm. However, in my view, taking nearly three months to provide notice is simply too long. I believe that Capital Health conscientiously followed-up on this incident; however, the lapse in time between the loss of the device and formal notification of affected individuals may illustrate a procedural or process flaw. For this reason I will recommend to Capital Health that they review their incident response procedure and processes to consider whether revisions would make the process more efficient without sacrificing due diligence.

¹ <http://www.capitalhealth.ca/NewsAndEvents/NewsReleases/2007/StolenLaptops.htm>

IV Application of HIA

[12] The *Health Information Act* (HIA) applies to “health information” in the custody or control of a “custodian”.

[13] Capital Health is a regional health authority and consequently falls within the HIA definition of “custodian” under section 1(1)(f)(iv).

[14] I have reviewed the report provided by Capital Health that describes the information held on the laptops. The information consisted of names, birth dates, addresses, personal health care number and, in some cases, the reason for visit to a Capital Health facility. This is “registration information” and “diagnostic, treatment and care information”. I find this is “health information”, as defined in section 1(1)(k) of HIA.

[15] I find the HIA applies to Capital Health, as a custodian with custody and control of health information.

V Issue

Did Capital Health fail to safeguard health information in contravention of section 60 of the *Health Information Act*?

VI Analysis

[16] Section 60 of HIA requires that reasonable steps be taken to protect health information. The relevant portions read:

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,

[17] The HIA requires that reasonable steps be taken to protect health information against reasonably anticipated threats. When a threat has been

identified, the steps taken to protect the information must include administrative, technical and physical safeguards.

[18] One way for a custodian to identify common threats is to review current trends and investigation reports released by the Information and Privacy Commissioner. The threat of a laptop being stolen is well known. The Commissioner has previously released two investigation reports that identified the threat and risk of storing health or personal information on a mobile device. In investigation report P2006-IR-005, the investigator said “Frequent incidents of laptop theft from employees, often despite corporate policies, are well known and publicized, making the risk real and foreseeable.” This threat was further reported in an investigation report (H2006-IR-002) concerning laptops stolen from the Calgary Health Region.

[19] Another way a threat can be identified is by completing a threat risk assessment. A properly conducted threat risk assessment will identify vulnerabilities and afford an organization an opportunity to make an informed decision about safeguards to implement to mitigate risk. It is not expected that a custodian provide fail-safe security, but reasonable steps must be taken to protect health information against anticipated threats. This first requires that some form of a risk assessment be completed.

[20] The practice of conducting risk assessments is supported by HIA *Health Information Regulation* (the Regulation) section 8(3), which requires a custodian to periodically assess its administrative, technical and physical safeguards. This is also an established best practice found in information security standards such as the International Organization for Standardization 17799 Code of Practice for Information Security Management.² With respect to use of mobile devices, the Code specifically says the “risks of working in an unprotected environment should be considered and appropriate protections applied.”³ Health regions in Alberta have been directed by the Minister of Alberta Health and Wellness to align to the ISO 17799 information security standard, and they are currently progressing through implementation of this standard.

[21] In summary, the HIA requires that a custodian take reasonable steps to maintain administrative, technical and physical safeguards to protect health information. A risk assessment must be conducted by a custodian to identify areas of risk, which provides the opportunity to determine appropriate safeguards to protect health information. I will examine each type of safeguard to assess whether Capital Health took reasonable steps to maintain safeguards.

Analysis of Safeguards

Administrative Safeguards

² International Organization for Standardization, Geneva, Code of practice for information security management, Reference number ISO/IEC 17799:2005(e), page ix.

³ Ibid, page 74.

[22] Policies and procedures serve as administrative safeguards, which are necessary to guide affiliates⁴ on steps that must be taken to protect health information. Policies and procedures are required by section 63 of HIA. Sections 60(1)(d) and 62(4) require a custodian to take reasonable steps to ensure it and its affiliates are aware of and comply with the policies and procedures established or adopted under section 63.

[23] The HIA requires that reasonable steps be taken to maintain safeguards. Maintenance of safeguards goes beyond simply having safeguards. The word “maintenance” implies that certain action is necessary. In my view, in order to maintain administrative safeguards, a custodian must take reasonable steps to implement, educate, ensure compliance with and periodically assess the ongoing effectiveness of the safeguards implemented. Therefore, in order to comply with the requirement to “maintain” administrative safeguards a custodian must:

1. Implement policies and procedures (section 63),
2. Educate affiliates on the policies and procedures (Regulation 8(6))
3. Ensure affiliates comply with the policies and procedures (section 62(4)), and
4. Periodically assess effectiveness of the policies and procedures (Regulation 8(3)).

[24] My investigation found Capital Health implemented organizational policies and procedures related to the privacy and security of health information, and generally has taken reasonable steps to educate and communicate them to affiliates. However, the information before me suggests that Capital Health did not periodically assess the effectiveness of their policies and procedures.

[25] Capital Health has a “Security of Equipment and Digital Storage Media” procedure that is dated June 17, 2002, which was last revised on July 14, 2003. The procedure provides guidelines for desktop and laptop security. Under the heading “Security of Laptops”, it says “Storage of health or personal information on portable equipment must be protected by secret password or encryption.” The procedure provides an option of encryption, but encryption is not required.

[26] The Commissioner released investigation report P2006-IR-005 on September 26, 2006 and report H2006-IR-002 on December 5, 2006. These reports addressed the safeguards required to protect personal or health information and recommended that personal or health information stored on a mobile device be encrypted. Investigation report H2006-IR-002 included specific comments to health information custodians. A number of recommendations were made to custodians, including “If you must store personal or health information on a

⁴ “affiliate”, in relation to a custodian, includes (i) an individual employed by the custodian, (ii) 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, and (iii) a health services provider who has the right to admit and treat patients at a hospital as defined in the *Hospitals Act*,

mobile device, use encryption to protect the data – password protection alone is not sufficient.”

[27] In September 2006 and again in December 2006, through release of the reports noted above, the Commissioner advised organizations and custodians they must encrypt personal or health information stored on a mobile device. Proper maintenance of safeguards requires periodic review and revision of policies and procedures to reflect current standards. Capital Health did not revise its policy or procedure to reflect the Commissioner’s instruction related to encryption. Therefore, I find that Capital Health did not properly maintain administrative safeguards to protect health information.

Technical Safeguards

[28] The technical safeguards implemented on the stolen laptops were a power-on and administrator password. It was established in Investigation Reports P2006-IR-005 and H2006-IR-002 that such passwords can be easily cracked or by-passed. These passwords are a safeguard that should be in place but, in and of themselves; do not provide a sufficient level of protection to meet the requirements of HIA.

[29] Our Office has recommended a layered defence to protect health or personal information stored on mobile devices. The defence must include properly implemented encryption in order to meet the requirements to safeguard health information under the HIA. The information on the laptops stolen from Capital Health was not encrypted.

[30] In an Edmonton Sun article responding to the stolen laptops, Capital Health was reported to say they had implemented software that locks the hard drives of laptops, which affords the same level of protection as encryption. However, drive-locking technology has no bearing in this incident as the stolen laptops did not have this system implemented. Furthermore, the Commissioner had previously established that the standard for protecting health or personal information stored on a mobile device is properly implemented encryption. Additional safeguards, such as software/hardware to lock hard drives may be implemented as part of a layered defence strategy to afford a higher level of protection. However, this should be done in addition to properly implemented encryption.

[31] Capital Health did not meet the requirement to periodically assess safeguards, and did not revise its policy related to encryption or take steps to implement an encryption solution for mobile devices. Therefore, I find that Capital Health did not maintain technical safeguards to protect health information.

Physical Safeguards

[32] The computers were stolen from a single story building in downtown Edmonton occupied only by Capital Health staff. The building has an alarm system, is only accessible with a security access card and is patrolled by security

staff in the evening. Security staff activates the alarm system later in the evening well after normal work hours and after staff had left the office. It is believed the computers were stolen after the last staff left the office, but before security activated the alarm.

[33] Staff had moved into this building approximately one month prior to this incident. Furniture with lockable cabinets, drawers or re-keying of existing furniture had been ordered, but had not yet arrived. The laptops were cable locked to desks. It is not known how the locks were pried off the laptops.

[34] It is well known that theft of laptops or other mobile devices is a foreseeable threat. The HIA requires that physical safeguards be maintained to protect health information against a reasonably anticipated threat. This means the device that holds health information must be physically secured. The standard required is one of reasonableness. That a determined thief can breach the physical safeguards in place does not necessarily mean the requirements of HIA were not met. In my view, a locked building, alarm system, access cards, security guards and cable locks are all reasonable physical safeguards. I find Capital Health met the requirements of the HIA to maintain physical safeguards to protect health information.

[35] Capital Health has reviewed the physical security at this site and decided that certain improvements will be made. I will not discuss these improvements in my report to ensure information is not inadvertently released that weakens the measures being taken.

VII Conclusion

[36] I have found that Capital Health did not maintain adequate administrative and technical safeguards. Therefore, I find Capital Health failed to safeguard health information in contravention of section 60 of the *Health Information Act*. However, it should be noted that Capital Health immediately began taking steps to address this matter, including reporting to the Information and Privacy Commissioner and fully cooperating in the investigation.

[37] To meet the minimum requirements to protect health information stored on a mobile device (eg. laptop, memory stick, PDA, data back-up disk or tape):

1. There must be policies and procedures that users are aware of and educated on that guide proper use of the device,
2. Reasonable steps must be taken to physically secure the device,
3. There must be a business need to store health information on the device,
4. The device must be password protected, and
5. Health information stored on the device must be protected by properly implemented encryption.

[38] A custodian is contravening the law if these minimum steps are not taken.

[39] During my investigation, Capital Health proceeded with an encryption deployment plan that includes the following:

- An RFP has been issued to acquire an appropriate encryption solution.
- Guidelines are being written to identify high risk laptops, which will be used to prioritize laptops that require encryption.
- Encryption will be implemented on all high risk laptops, which are those that contain personal or health information, beginning in January 2008.
- In the interim, a solution that locks hard drives will be deployed on all laptops.

VIII Recommendations

[40] I make the following recommendations to Capital Health:

1. Capital Health proceed with its plan to issue an RFP, select an appropriate encryption solution and begin implementation on a priority basis,
2. Capital Health ensure its plan includes identification and proper implementation of encryption on all types of mobile devices that contain personal or health information,
3. Capital Health provide our Office with a detailed implementation plan that includes aggressive targets and timelines for our consideration, and
4. Capital Health review and revise as necessary its incident response procedure, and in particular, its process to notify patients of privacy breaches.

[41] Capital Health has agreed to these recommendations and committed to taking the steps necessary to ensure health information on mobile devices is properly safeguarded.

Submitted by

LeRoy Brower
Director, Health Information Act