

INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA

Investigation Report Concerning a Stolen Laptop Containing Health Information

October 21, 2008

East Central Health

Investigation Report H2008-IR-003

(Investigation H2200)

Introduction

[1] On August 5, 2008, East Central Health (ECH or “the Region”) informed the Information and Privacy Commissioner (the Commissioner) that a laptop containing health information had been stolen from the Two Hills Health Centre.

[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.

Background

[3] On July 21, 2008, a laptop computer was stolen from the Two Hills Health Centre Diagnostic Imaging Unit. The laptop was used to capture and store digital echocardiogram¹ (digital ECG) images. A digital ECG differs from a traditional ECG in that the graph of cardiac function is stored in an electronic file format as opposed to being recorded on paper. The laptop computer that was stolen was also used to email files containing the digital ECGs to a radiologist to interpret and to store the final reports. The email that accompanies a digital ECG includes the patient’s first and last name, gender, date of birth, a patient identification number and any other information that could impact the reliability or validity of the ECG (such as cardiac risk factors or medications).

[4] At the time the laptop was stolen, it contained the health information of the 1506 individuals who had had this procedure done since ECH adopted the use of digital ECGs in 2006.

[5] Staff at the Two Hills Health Centre reported the theft of the laptop to the police immediately on noticing that the cable used to secure the laptop to the ECG workstation in the Diagnostic Imaging Unit had been cut and the device

¹ An ECG is a diagnostic test used to monitor electronic potential (stimulation) of the heart over time.

was missing. They also identified an individual who had been loitering in the area to the police as a potential suspect. The laptop was recovered by the police and returned to the facility within one hour.

[6] ECH wrote to our Office on July 29, 2008, and advised us that it had elected not to notify the affected individuals for the following reasons:

- The laptop hard drive was encrypted
- The laptop was only out of their possession for a period of one hour
- The level of risk that information could have been accessed was, in their opinion, extremely low given the full disk encryption on the device and the limited time it was out of their possession

Application of the Health Information Act

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

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

[9] I have reviewed the report provided by ECH, which included a copy of a previously conducted privacy impact assessment on the project that laid out the health information contained that would be stored on the laptop. The information consists of patient first and last name, gender, date of birth, a patient identification number, other relevant health information and a digital copy of the patient’s ECG. This is “registration information” and “diagnostic treatment and care information” as defined in sections 1(1)(u) and 1(1)(i) of the HIA. This is “health information” as defined in section 1(1)(k) of the HIA.

[10] As the information at issue is health information and ECH is a custodian, I find that the HIA applies.

Issue

[11] Did ECH fail to safeguard health information in contravention of section 60 of the *Health Information Act*?

Analysis

[12] Section 60 of the HIA requires a custodian to take reasonable steps to protect health information. The relevant sections 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...

(3) In subsection (2)(a), "electronic health records" means records of health information in electronic form.

[13] Several of my colleagues have considered the protection of health information stored on mobile devices, including laptops. The key findings of Investigation Reports H2006-IR-002 and H2007-IR-002 are:

1. Custodians must assess the privacy and security risks associated with the use of mobile devices and should limit the use of these devices to circumstances where mobility/portability is required (i.e. cannot be achieved through any other means).
2. Health information that is stored on a mobile device must be protected by properly implemented encryption.
3. Custodians must take reasonable steps to physically secure mobile devices, even when encrypted.
4. Custodians that store health information on mobile devices must implement policies and procedures that users are aware of and educated on that guide the proper use of the device.

[14] The combination of these administrative, physical and technological safeguards creates a reasonable standard of protection when health information is stored on mobile devices. The failure to include one of these elements leaves health information unacceptably vulnerable to loss, theft and unauthorized disclosure.

[15] I must now assess whether or not ECH met these standards.

Did ECH assess the privacy and security risks associated with the use of a laptop as part of the Digital ECH program?

[16] Section 64 of the HIA requires custodians to prepare a privacy impact assessment (PIA) that describes how proposed administrative practices or information systems relating to the collection, use and disclosure of health information may affect the privacy of individuals.

[17] ECH completed a PIA on the "Digital Electrocardiogram System (Rapid Read ECG System)" and submitted it to the Information and Privacy Commissioner for review and comment on November 3, 2006. The PIA was accepted on August 29, 2007.

[18] One of the fundamental elements of a PIA is development and articulation of a privacy risk assessment and mitigation strategy. Through this

process, custodians identify where reasonably anticipated risks to privacy exist for a particular project and describe the technical, physical and administrative safeguards they will use to minimize the likelihood and/or consequence of a privacy breach.

[19] ECGs are often, particularly in emergency departments, performed at the patient's bed. Ill patients are not moved into a specified location to have an ECG performed; the ECG workstation is moved to the area where treatment and care is provided. In the case of digital capture of ECG results, this translates into a requirement that the storage device (the laptop computer) be mobile as well.

[20] ECH identified through the PIA process that the use of a laptop computer as part of this program increased the likelihood of the theft the laptop and the consequential unauthorized disclosure of health information. To mitigate against this increased risk, ECH took the following steps:

- Deployment of full disk encryption on the Digital ECG program laptops
- Creation of a requirement that the Digital ECG program laptops be secured to the ECG cart and that the cart be stored in a non-public area

[21] ECH assessed the privacy and security requirements of the use of laptops as part of the Digital ECG program through the PIA it submitted in November 2006. As such, it fulfilled its obligation to identify and assess privacy risk as required by section 64 of the HIA and met the first criteria for protection of health information stored on a mobile device.

Did ECH properly encrypt health information store on the laptop?

[22] The Digital ECG laptop hard drive was encrypted by the system vendor using industry recognized encryption software prior to being used in the provision of health services. When the laptop was returned to the Region, Information Technology staff conducted a technical inspection of the device and confirmed that the encryption software was functioning as expected.

[23] By encrypting the laptop and taking steps to ensure that the software was functioning as expected, ECH met the second criteria for protection of health information stored on a mobile device

Did ECH take reasonable steps to physically secure the laptop?

[24] In this case, the laptop computer was physically attached to a digital ECG mobile workstation using a regionally approved cable lock. The digital ECG workstation was stored in the Diagnostic Imaging (DI) area of the health centre, which is locked when staff are not physically present.

[25] Despite these safeguards, the laptop computer was still stolen. The individual who stole the computer had noticed the laptop in the DI area earlier in the day and returned with wire cutters. When the staff member who was supervising the DI area was briefly drawn to another area of the unit to attend

to a patient, the individual cut the laptop cable and took the device. The theft was noticed by the staff member when she returned to the central DI area and immediately reported to police. The laptop was recovered by police and returned to the hospital within the hour.

[26] The combination of the physical cable lock, the supervision of a staff member and the locking of the unit doors when not supervised are, in my opinion, reasonable steps to secure a laptop computer. ECH thereby met the third criteria for protection of health information stored on a mobile device

Did ECH implement policies and procedures that users are aware of and educated on that guide the proper use of the device?

[27] ECH has information security policies and procedures. I have reviewed these policies and procedures and find that they do not expressly require that the hard drives of laptops containing health information be encrypted. That being said, ECH has developed a number of "ad hoc" controls in the absence of express policy direction on this point. During my investigation, ECH described a number of processes that have been adopted in relation to encryption including training and the control of encrypted devices, but these processes have not been integrated into policy.

[28] ECH has been aware of the need to revise its information security policies and procedures for some time and has, in collaboration with other health regions, drafted a revised policy set to close the gaps they have identified. It is my opinion that the draft policies and procedures are a significant enhancement to the current policies and procedures in relation to the requirement for encryption on mobile devices. The draft policy expressly states that mobile computing devices must store minimal information and that any information stored on mobile computing devices must be password protected and encrypted. ECH has advised me that these policies are expected to be approved by region management in mid-October.

[29] As the policy and procedures currently in place in ECH does not require the encryption of mobile devices, ECH did not meet the final requirement. That being said, ECH has developed a draft policy set that will meet this requirement when it is approved in mid-October 2008.

Notice to Affected Individuals

[30] When ECH notified our office of the theft of the Digital ECG laptop, it indicated that it had assessed the risk of harm to affected individuals as so low that notification would not be required.

[31] Our Office has previously taken the position that individuals should be notified of privacy breaches where there is a potential for harm resulting from the unauthorized disclosure of personal and/or health information.

[32] It is my opinion that the fulsome implementation of encryption software in this case reduces the likelihood that health information was accessed and

disclosed in contravention of the HIA to an extremely low level. I agree with ECH that notification of the affected individuals would serve no practical purpose.

Conclusion

[33] ECH has taken many steps to protect health information that must be stored on laptop computers. These steps include conducting a risk assessment prior to using mobile devices, ensuring that mobile devices that store health information are encrypted and that they also adhere to minimum regional standards related to physical security and passwords. ECH has also recognized the need to support these practices through the development of policies and procedures and has drafted policies that give force and effect to these essential privacy and security controls.

[34] By way of closing comment in this case, I wish to commend ECH for its proactive management of this issue from the privacy impact assessment phase through to voluntarily advising our office of a potential privacy breach involving the Digital ECG program. The Region has been responsive to the recommendations I made through the investigation and remains committed to strengthening its information security program.

Submitted by:

Leahann McElveen
Portfolio Officer, Health Information Act