

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

Report on Investigation into Missing Computer Tape Containing Health Information

June 30, 2005

**Alberta Health and Wellness
(Investigation # H0725)**

Investigation Report H2005-IR-001

I. INTRODUCTION

[1] On March 11, 2005, Alberta Health and Wellness (AHW) notified this Office that a data tape containing the information of a large number of Albertans was missing.

[2] In response to the notification provided by AHW, the Commissioner initiated an investigation on his own motion under section 84(a) of the *Health Information Act* (HIA). Section 84(a) authorizes the Commissioner to conduct investigations to ensure compliance with any provision of the HIA.

II. INFORMATION AT ISSUE

[3] The missing data tape contains information related to the administration of the Alberta Health Care Insurance Plan (AHCIP), specifically, group premium statement information. AHW states that the tape could include information about any individual whose employer and other agencies send monthly health care premiums on their behalf.¹

[4] AHW says the data tape contained information about 672,316 individuals. The information on the tape with respect to each individual consists of:

- name, personal health number and department/employee number (where applicable)
- monthly health care premium rate and changes to the rate
- family status, number of dependants

[5] “Health information” is defined in section 1(1)(k) of the HIA and reads as follows:

“health information” means any or all of the following:

- (i) diagnostic, treatment and care information;*

¹ Including government sponsored organization, union or other organization that collects premiums on behalf of their members.

- (ii) *health services provider information;*
- (iii) *registration information;*

[6] Section 1(1)(u) of the HIA defines “registration information”. Registration information includes demographic, health service eligibility and billing information relating to an individual.²

[7] I find that the information on the data tape is “registration information” and is therefore “health information”. There is no “diagnostic, treatment and care information” or “health services provider” information on the data tape.

III. BACKGROUND

[8] In September of 2000, AHW re-negotiated an outsourcing agreement with IBM Canada Ltd. (IBM). The agreement is to provide information technology services to AHW. The agreement requires IBM to store “health information” on its mainframe computer at IBM’s Calgary data centre. The “health information” is sent by AHW to IBM via secure file transfer protocol via the internet. IBM backs up the “health information” held on its mainframe onto magnetic data tapes. These tapes are kept in a tape library. IBM’s mainframe tape library includes approximately 19,000 AHW tapes. 400 of these tapes are used specifically to move information to other vendors or recipients as directed by AHW. All tapes are labeled with a unique serial number and a ‘return to’ address for the IBM Calgary data centre. In September of 2004, IBM conducted a physical inventory and all tapes were accounted for.

[9] One of the services IBM provides under the outsourcing agreement is to copy AHCIP group premium statement information from the mainframe to one of the 400 data tapes. When the tape has been created, IBM sends it by private courier to a microfiche vendor located in Edmonton.

[10] The microfiche vendor creates microfiche under an agreement with WNS Emergent Inc. (now CriticalControl Solutions Inc.) who holds a government-wide imaging services agreement that was signed in September of 2003. Part of this government-wide agreement is to transfer AHCIP group premium statement information onto microfiche.

[11] The microfiche vendor converts the information held on the tape to microfiche. Microfiche is a page of film containing images of records from the tape that is created for archival and information retrieval purposes. Once the microfiche has been created, the microfiche vendor returns the tape by private courier back to IBM in Calgary. This occurs approximately three times a month. The microfiche vendor hand delivers the microfiche to CriticalControl Solutions Inc. (Critical Control) who stores it for archival and information retrieval purposes.

²Demographic information includes an individual’s name, signature, photograph or electronic image, personal health number or any other unique identification number used to identify an individual as eligible for or a recipient of a health service, gender, date of birth, birth information, marital status, date of death, treaty status and band number (HIA Regulation 3(a)).

[12] The following describes the standard process for creation and disposition of a data tape produced for the purpose of creating microfiche:

- The IBM data centre holds data tapes in a data tape library.
- The data tapes remain in the library until the Removable Media Manager (RMM) identifies a tape by serial number to be returned to the tape pool for re-use, for example, to back-up the “health information” held on the mainframe. The RMM is an automated tape library management system.
- IBM then transfers the AHCIP group premium statement information onto the tape identified by the RMM.
- IBM Calgary places the data tape in a plastic container or bubble wrapped envelope and ships it by private courier from their Calgary data centre to the microfiche vendor in Edmonton. A computer printout, listing the serial number of the data tape included in the shipment, is placed in the plastic container or bubble wrap envelope.
- The microfiche vendor creates the microfiche.
- The created microfiche is hand delivered by the microfiche vendor to Critical Control in Edmonton, who stores it for archival and information retrieval purposes.
- The microfiche vendor ships the data tape back to IBM’s data centre in Calgary via private courier.
- IBM returns the data tape to their tape library.

Chronology

[13] On December 20, 2004, IBM sent the data tape at issue from their Calgary data centre in Calgary by private courier to the microfiche vendor in Edmonton. The tape was shipped in a plastic container. A computer printout, listing the serial number of the tape included in the shipment, accompanied the tape.

[14] The data tape was received by the microfiche vendor and microfiche was processed. The microfiche was delivered by the microfiche vendor to Critical Control.

[15] The microfiche vendor said that on December 21, 2004, he returned the data tape at issue to IBM’s data centre in Calgary in one of four plastic containers sent in that shipment. These are the same plastic containers used by IBM to ship the tapes back and forth to the microfiche vendor. The microfiche vendor produced a courier bill of lading to show that four containers of data tapes had been returned to IBM Calgary on December 21st.

[16] IBM confirmed to me that it did receive four plastic containers returned by the microfiche vendor, all of which contained data tapes.

[17] On February 17, 2005, the RMM called for the AHW data tape to be returned to the tape pool. The librarian could not locate the tape in the tape library.

[18] From February 18 to March 3, 2005, IBM conducted searches for the missing data tape. After concluding that the tape was lost, IBM notified AHW on March 4, 2005.

[19] From March 4 to March 17, 2005, IBM took a number of additional steps in an effort to locate the missing data tape. These steps included a number of searches of the IBM data centre and tape library; searches of IBM mailrooms and loading docks in Edmonton and Calgary, IBM office areas, shipping and receiving, labs and communications areas, kitchens, reception area, microfiche and storage and meeting rooms, IBM's off-site tape storage location; search of the private sector courier locations in Calgary, Edmonton and the courier's lost and found depot in Toronto; and search of the microfiche vendor in Edmonton.

[20] On March 14, 2005, AHW suspended microfiche tape movement while they reviewed related processes and examined safeguards.

IV. APPLICATION OF THE HIA

[21] The HIA applies to "health information" in the custody and control of a "custodian", which includes AHW and other health service providers paid for the provision of health services under the Alberta Health Care Insurance Plan.

[22] I have found that the information on the missing data tape is "health information". The "health information" on the missing data tape was in the custody or under the control of AHW.

[23] This incident involves two information managers³ for AHW.

[24] IBM provides information management and technology services for AHW, and is therefore an information manager as set out in section 66(1).

[25] As Critical Control provides information management services for AHW under a government-wide imaging services agreement, it is also an information manager for AHW. Critical Control sub-contracts a microfiche vendor to transfer AHCIP group premium statement information from a data tape to microfiche.

[26] Section 60 of the HIA requires a custodian to protect health information. The relevant portion of section 60 reads 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

³ An information manager means a person or body that a) processes, stores, retrieves or disposes of health information, b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, and c) provides information management or technology services (HIA section 66(1)).

(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.*

[27] Section 66 of the HIA says that a custodian may enter an agreement with an information manager to provide information management services. The responsibility to protect the “health information” disclosed to the information manager is set out as follows:

66(5) An information manager must comply with

(a) this Act and the regulations, and

(b) the agreement entered into with a custodian

in respect of information disclosed to it pursuant to subsection (3).

(6) Despite subsection 5(a), a custodian continues to be responsible for compliance with this Act and the regulations in respect of the information disclosed by the custodian to the information manager.

[28] AHW therefore must take reasonable steps to ensure compliance with the HIA by itself and its information managers.

V. Findings

Shipment of individual data tapes not tracked

[29] IBM sent the missing data tape to the microfiche vendor by a private sector courier in a plastic container with a computer printout listing of the tape included in that shipment.

[30] The microfiche vendor received the data tape and created the microfiche. I have viewed pages of the microfiche and confirmed that the information contained on the missing tape is as previously described. This confirms that the microfiche vendor did receive the tape from IBM. The microfiche vendor then hand delivered the microfiche to Critical Control.

[31] The microfiche vendor said that the missing data tape was returned to the IBM data centre in Calgary in one of four plastic containers. The microfiche vendor did not include a listing of the individual tapes being returned in each container, and therefore could not confirm that the AHW tape was included in the shipment. The courier bill of lading shows that four containers were returned to IBM, but does not identify the contents of the containers. Consequently, the microfiche vendor could not provide me with conclusive evidence that the data tape had been returned.

[32] Upon receipt of the four containers of data tapes, IBM returned the tapes to its tape library in the Calgary data centre. IBM did not track receipt of the individual tapes returned by the microfiche vendor in each container, nor was there verification with the microfiche vendor as to what tapes had been returned. IBM could confirm that they received four plastic containers of tapes, but not whether they had received the missing AHW tape. IBM could not confirm which tapes were in any specific container. Consequently, IBM could not provide me with evidence that they did or did not receive the missing tape from the microfiche vendor.

[33] As there was no tracking of individual data tapes (just of the containers), I have been unable to identify the location where the data tape may have been lost. I therefore cannot identify who is responsible for the loss.

[34] IBM's internal investigation identified the need for better controls in tracking computer tape movement. As a direct result of this incident, IBM initiated the following changes to its tape movement procedure:

- IBM continues to include a computer printout listing of the computer tapes in the package that is sent to the microfiche vendor. In addition, IBM sends an email message to the microfiche vendor that a package is being sent. The email message also contains the courier waybill number, the number of computer tapes being sent and a listing of each computer tape.
- The microfiche vendor is required to send an email reply to IBM confirming receipt of the tapes.
- When returning the computer tapes to IBM, the microfiche vendor is required to send an email to IBM stating which computer tapes are being returned, the number of containers being returned and the courier waybill number.
- Upon receipt of the package from the courier, IBM verifies the contents of the package with the information provided by the microfiche vendor to ensure that all computer tapes are accounted for.
- IBM will conduct a weekly accounting of all outstanding computer tapes. This will enable IBM to identify unaccounted computer tapes prior to their re-use (which may be 30 or 60 days dependent upon the established schedules).

[35] AHW subsequently decided to stop creating microfiche of the AHCIP group premium statement information. Therefore, the data tapes used in this tape movement process are no longer being shipped.

Plastic containers used to ship data tapes not secure

[36] The plastic containers used to transport data tapes via courier from IBM to the microfiche vendor and back to IBM are not sealed in a manner that would restrict access or demonstrate whether the container had been tampered with.

[37] Every precaution should be exercised when determining the level of security to apply in transporting “health information” by courier. This incident involves a planned and regular shipment between two parties of an information medium that contains thousands of individuals’ “health information”. In my view, these circumstances require an increased level of security that may not be required for single irregular shipments.

Timeliness of notice to AHW

[38] The agreement between AHW and IBM requires IBM to “notify the Minister promptly if it becomes aware or has reasonable grounds to suspect that unauthorized disclosure of Minister’s Confidential Information has occurred”. IBM first learned that an AHW data tape was missing on February 17, 2005. IBM notified AHW on March 4th, which is 11 working days later. While it is understandable that IBM would conduct searches to confirm that the tape was lost and conduct internal investigations, it is my opinion that IBM should have notified AHW within 48 hours of being unable to locate the tape.

No contract to create microfiche

[39] Creation of microfiche is one small part of the government-wide imaging services agreement. Critical Control sub-contracted this service to the microfiche vendor; however, there is no written agreement setting out accountabilities and privacy and security requirements between Critical Control and the microfiche vendor. This seems to have been an oversight due to a long standing arrangement with the microfiche vendor that pre-dates the imaging services contract.

VI. Risk to Albertans

[40] In this incident, I have considered three questions in assessing the level of risk associated with the loss of the data tape:

1. Has the data tape been found by someone?
2. Can the “health information” be extracted from the data tape?
3. Is the “health information” on the tape information that may be used for fraudulent or otherwise harmful purposes?

[41] If the answer to any of these questions is no, the risk to Albertans is significantly reduced. For example, if the tape remains wherever it is now and has not been found by anyone, there is no possibility that information has been extracted. There is risk only if the tape is found by someone with the means and desire to extract the information. The risk increases if the tape has been found; the information on the tape is accessible and is the kind of information which is useful for fraudulent purposes.

[42] I will consider each question in turn.

Has the Tape Been Found?

[43] Extensive searches by IBM, the private sector courier and the microfiche vendor have failed to locate the data tape and its location remains unknown. The tape may simply be lost, may have been disposed of, or in a location where it will never be found. More than 4 months have now elapsed since the tape was discovered missing. We have not received any information that the data tape has been found or is in the hands of an unauthorized person.

Can the “Health Information” be Extracted?

[44] Deloitte & Touche Forensic and Investigative Services Inc. (Deloitte) was contracted to provide an analysis of a like data tape to assist in determining if it is possible to extract data from the missing tape. Relevant portions of Deloitte’s assessment are as follows:

- in order to access this kind of tape, a compatible tape drive is required
- once you have a compatible tape drive, any personal computer system is capable of restoring the data from the tape, as long as it is equipped with an interface card necessary to connect the computer to the tape drive
- a refurbished compatible tape drive can be purchased through the Internet for approximately \$2500 US, and may be purchased through auction or clearing houses for considerably less
- an interface card can be purchased for approximately \$350
- five different methodologies were utilized to demonstrate the variety of methods to retrieve usable data from the tape with varying degrees of cost, skill level and equipment requirements
- access to and conversion of the data contained on the tape was quickly accomplished resulting in readable/usable data

[45] Deloitte has shown that the information on the tape is accessible. While a specialized tape drive compatible with the type of the missing data tape would be required, along with software that (for security reasons) I have chosen not to describe here, compatible drives are available for purchase and may be sold with the software necessary to extract the information. However, this presumes that an individual who finds the tape is able to determine what type of tape it is, and has the motivation and means to take the steps necessary to access the information.

Is the “Health Information” Useful for Fraudulent Purposes?

[46] The tape contains information related to the administration of the AHCIP. The information includes an individual’s name, personal health number, department/employee number, monthly health care premium rate, family status and number of dependants. It does not contain diagnostic and treatment health information.

[47] As the data tape does not contain credit information, its usefulness for fraudulent purposes is limited. However, it may be possible to use the information on the tape to fraudulently obtain health care services, or the information could be used to pose as the individual the information is about in an attempt to obtain additional information that could be used to commit fraud.

[48] In September 2004, the Auditor General recommended that AHW improve control over the issuance of replacement Personal Health Cards and the health registration system. AHW has progressed in implementing these recommendations and continues to work with the Office of the Auditor General to address this issue. The steps taken by AHW to tighten security controls reduces the risk that someone could use the information on the data tape for fraudulent purposes related to the health care system or to fraudulently obtain a replacement Personal Health Card. The first line of defense in preventing misuse of the information on this tape will be AHW's security controls.

Summary of Risk

[49] Based on the "health information" on the tape and the likelihood of the tape being found and read, I have assessed the risk to individuals as being low. The risk arises from the possibility that someone will use the information to fraudulently obtain health care services, obtain a duplicate Personal Health Card that could then be used to support an identity theft or to seek out additional information useful to commit fraud. While the tape probably remains lost, there is a possibility that it either has been or could be found in the future. I am also conscious that it is possible to extract the information on the tape once a compatible tape drive has been acquired. The overall risk is reduced because of the steps being taken by AHW to implement the Auditor General's recommendations. The analysis of risk is relevant to deciding what kind of notice AHW should provide to Albertans.

[50] Our Office has previously required or worked with organizations to determine notice requirements to individuals who may be affected by a breach of privacy. In investigation report F2005-IR-002, the Alberta Pensions Administration Corporation directly notified all affected parties following the loss of four computer data tapes and two pages of microfiche. In investigation reports P2005-IR-001, P2005-IR-002 and P2005-IR-003, organizations were required to provide notice to affected individuals in circumstances where information had been exposed to fraud, and where information may have been exposed to fraud.

[51] There is no information before me to confirm or even suggest that the information on the missing data tape has been exposed or used for fraudulent purposes. Nevertheless, fraudulent use remains a possibility until the data tape is located and returned to AHW. AHW should therefore take steps to notify all affected Albertans. In my view, substitute notice is appropriate given the level of risk and the large number of affected individuals and this is reflected in my recommendations.

VII. CONCLUSIONS

[52] I have found that individual data tapes were not tracked, and that an increased level of security should be applied to planned and regular shipments of “health information”. I do not believe that tracking of individual tapes would have prevented the loss of the tape, but it would have led to an earlier determination that a tape had been lost and identified the location of the loss, which would have increased the likelihood of finding the tape. Although there is no evidence that the plastic container was tampered with, only a secured container could conclusively demonstrate that it was secure. Finally, while a written agreement between Critical Control and the microfiche vendor should have been in place, the fact that there was no agreement was not a factor in this incident.

[53] When considering whether AHW met requirements of the HIA to maintain safeguards to protect health information, I have considered both the areas where improvements could be made and the efforts of AHW to ensure the right safeguards were in place. The steps taken by AHW to maintain administrative, technical and physical safeguards include:

- completion of a security Information Management/Information Technology framework that is incorporated into and forms part of the agreement with IBM,
- development of security policies and procedures that are incorporated into and form part of the agreement with IBM,
- annual review of the security policies and procedures that are incorporated into and form part of the agreement with IBM,
- monthly security working group meetings that include the AHW Security Office, AHW IT Operations, AHW Security Contractors and AHW vendors, one of which is IBM, and
- independent SysTrust audit undertaken in 2004 that found that AHW maintained effective controls over the reliability of the outsourced systems that were part of the audit, which included the services outsourced to IBM

[54] Section 60 of the HIA requires a custodian to take “reasonable” steps to maintain safeguards to protect against a reasonably anticipated risk. It is not required or expected that a custodian foresee every incident that could occur. Required safeguards can be maintained and something may still go wrong. I find that AHW and its information managers have met the requirements of the HIA in this regard.

[55] As previously noted, AHW advised me they have stopped creating microfiche of the AHCIP group premium statement information, and therefore the data tapes used in this process are no longer being shipped. This operational change eliminates the risk of losing a tape and resolves the contractual issue. As such, I no longer have recommendations in relation to microfiche tape movement and related safeguards.

VIII. RECOMMENDATIONS

1. That AHW provide substitute notice to Albertans through the media (Edmonton Journal, Calgary Herald etc.) within 7 working days of this news release and post the notice in a prominent and highly visible location on the AHW website for a period of 30 days. The notice should include:
 - a general description of what happened
 - the nature of the individual's "health information" involved
 - what AHW has done to protect the individual's "health information" from a further security breach
 - an AHW contact telephone number where information and assistance can be provided to individuals who are concerned that their information may be used for fraudulent purposes
2. That AHW and IBM clarify the requirements regarding timelines for notification of privacy breaches, and update the contract accordingly.

Submitted by,

LeRoy Brower
Director, Health Information Act