OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

INVESTIGATION REPORT F08-02

MINISTRY OF HEALTH

David Loukidelis, Information and Privacy Commissioner

May 7, 2008

Quicklaw Cite: [2008] B.C.I.P.C.D. No. 16
Document URL: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF08-02.pdf

Summary: Four computer tapes containing personal information of residents of British Columbia and New Brunswick who received medical services outside their home province was couriered from New Brunswick to Health Insurance BC, a contractor for the Ministry of Health in British Columbia. They never arrived at HIBC. The information was on magnetic tapes and was not protected by encryption. This method of transferring personal information did not meet the security measures required under s. 30 of the *Freedom of Information and Protection of Privacy Act*. The Ministry's policies and practices resulted in failure to ensure the tape loss was detected in a timely way. The Ministry also failed to notify affected individuals and the OIPC in a timely way. After the loss was discovered, the Ministry took appropriate action to mitigate risk to the affected individuals. After the incident, the Ministry ceased exchanging unencrypted personal information of this kind with other jurisdictions. New Ministry procedures now monitor more closely such exchanges of personal information and the Ministry continues to work towards an even more secure method of data transfer.

TABLE OF CONTENTS

1.0 INTRODUCTION

[1] A shipment from New Brunswick to British Columbia of four magnetic computer tapes containing personal information of individuals who had received medical services in Canada outside of their home province did not arrive as expected. The fact that the shipment was overdue was not noticed until three weeks after it left New Brunswick. Two months after the tapes went missing, the Ministry of Health ("Ministry") notified the Office of the Information and Privacy Commissioner for British Columbia ("OIPC") of the tapes' loss. This is the report of the ensuing investigation by the OIPC, under s. 42 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA").[1] A separate, but related, investigation into the loss of personal information under the control of the New Brunswick Department of Health ("New Brunswick Department") has been conducted by the Office of the Ombudsman of New Brunswick. That report is being released concurrently with this report.

2.0 BACKGROUND

[2] To comply with the *Canada Health Act,* the Medical Services Commission of British Columbia, on behalf of the Ministry, has entered into reciprocal agreements to facilitate the sharing of heath care information with each of the provinces and territories of Canada other than Quebec, with Health Canada (respecting aboriginal people with status under the *Indian Act*), and with Citizenship and Immigration Canada (regarding indigent immigrants). The majority of the agreements came into effect in 1988, but some date back to 1981. Most call for information about insured persons who received medical services outside of their home province or territory to be provided to the medical services insurance plan in the home jurisdiction either "electronically", on "magnetic tape" or "in writing". Reimbursement for services is then made to the province or territory which provided the medical services.

[3] The Ministry indicated that, before this incident, information was shared between British Columbia and other Canadian jurisdictions using a variety of methods:

- PEI - paper records (courier)
- Nova Scotia - secure internet gateway
- New Brunswick - unencrypted magnetic tapes (courier)
- Newfoundland - unencrypted magnetic tapes (courier)
- Ontario - unencrypted magnetic tapes (courier)
- Manitoba - unencrypted magnetic tapes (courier)
- Alberta - unencrypted magnetic tapes (courier)
- Saskatchewan - encrypted CD (courier)
- Yukon - paper records or magnetic tape (courier)
- NWT & Nunavut - paper records (mailed) and secure FTP (file transfer protocol)

[1] This report contains findings and recommendations, but makes no order under s. 58.

[4] The information sharing agreement between British Columbia and New Brunswick came into effect on April 1, 1988. Section 3(6) reads as follows:

> The Host Province shall issue monthly statements to the Province of Origin, with magnetic tape, in the form attached as Schedule "B", or in writing, in the form attached as schedule "C".

[5] On October 3, 2007, an employee of X-Wave (the company which processes health insurance billing as a contractor to the New Brunswick Department) packaged four computer tape cartridges into a bubble envelope addressed to Health Insurance BC ("HIBC"), which administers the Medical Services Plan and PharmaCare in British Columbia. X-Wave turned the package over to Sameday RightOWay Courier ("Sameday Courier") for shipment to British Columbia. One of the tapes contained personal information of 124 British Columbia residents who had received health services in New Brunswick. This personal information was collected by and was under the control of the New Brunswick Department. The other three tapes contained information of 485 New Brunswick residents who had received medical services in British Columbia and the practitioner numbers of 570 British Columbia medical practitioners who provided the services. This personal information had been collected by the Ministry and was under its control.

[6] The following chronology outlines what happened next:

- October 25, 2007—HIBC contacted Sameday Courier enquiring as to the whereabouts of the routinely shipped tapes. Sameday Courier checked and responded that it could not locate the package. HIBC then contacted the New Brunswick Department to advise that the package had not arrived and had gone astray in transit.
- October 26, 2007—New Brunswick Department advised X-Wave to create a replacement tape with the information of the British Columbia residents and ship it to British Columbia.
- October 29, 2007—the Privacy Officer for HIBC was notified that the tapes containing personal information had gone missing and could not be located.
- October 29, 2007—HIBC notified the Ministry's Business Management Office of the possible privacy breach and that office then notified the Ministry's Director, Corporate Information, Privacy and Records.
- November 1, 2007—the accounts for each of the affected individuals who were British Columbia residents and could be identified at that time were flagged in the registration and premium billing database at HIBC. (Flagging these records results in anyone seeking medical services who cannot produce an MSP CareCard being required to produce identification before services will be provided.)
- October 30 to December 10, 2007—the Ministry was in communication with the New Brunswick Department to determine the size and nature of the potential privacy

breach. Discussions were held on the best way to notify the affected individuals. Initial plans were for joint notification of all affected individuals from both provinces.

- December 10, 2007—the Ministry notified this Office of the potential privacy breach. The Ministry and the New Brunswick Department agreed that British Columbia would be responsible for contacting the affected individuals who were covered by the MSP and the New Brunswick Department would contact the New Brunswick residents.
- December 11, 2007—the OIPC advised the Ministry that it should immediately send the planned notification letter to each of the 124 British Columbia residents whose personal information was on the missing tape. The Ministry also offered these individuals the option of obtaining a credit report or having an alert placed on their credit file, for which the Ministry would reimburse the costs up to $200.00. The Ministry agreed to cover the costs of obtaining the services of a credit monitoring agency. The Ministry also ceased the transmission of unencrypted health information which contains any personal information to other provinces/territories.
- December 17, 2007—Sameday Courier completed its investigation regarding the missing package. Sameday Courier was able to confirm that the package arrived at its Richmond depot at 7:14 a.m. on October 5, 2007. Sameday Courier advised that normally the next scan for this package should have been in Victoria on Monday, October 8.

[7] Sameday Courier advised X-Wave (the shipper) that as part of its investigation, it made the following efforts to account for the package:

- Its terminals in Richmond and Victoria were searched twice for the package.
- These terminals contacted their agent service providers to conduct searches for the missing package. All agents responded in the negative.
- Agent line haul carriers were contacted to search their premises for the package. Negative response was received.
- Undeliverable packages are forwarded to Sameday Courier's Overgoods Department where the packages are opened and attempts are made to identify the shipper or the intended recipient. This department was searched initially and then again when pictures of the tape cartridges were received. The package could not be located here.
- The Richmond Detachment of the RCMP had been contacted by the New Brunswick Department and attended at the Richmond terminal. Police found no evidence indicating the package had been stolen.

[8] Sameday Courier concluded that the package probably did not make it onto the truck going to Victoria from Richmond. The package either disappeared within the Richmond depot or was loaded onto a truck destined elsewhere. As of the date of this report, the missing tapes have not been located.

[9] The personal information involved consisted of name, gender, personal health number ("PHN") and birth date. It also included the fee code for the medical services each individual received and the practitioner number of the service provider.

[10] This personal information was recorded on four magnetic tape cartridges. Although the technology to encrypt the tapes was available by March 2007, it was not the practice of either government to do this. The magnetic tape cartridges are a somewhat dated technology and the equipment used to read them is typically only associated with large mainframe computers. According to the Ministry, hardware and software to read the data contained on such tapes is not readily available.

[11] When HIBC ships records out of British Columbia, it uses the "Rush & Trace" service of BC Mail, the government's in-house mail service. BC Mail uses Canada Post Priority courier service for deliveries in Canada going outside of British Columbia and the "Rush & Trace" designation requires signatures at all transfers of the package. New Brunswick ships packages to British Columbia using bonded nation-wide courier services, in this instance, Sameday Courier.

[12] Of the four lost tapes, one contained personal information of British Columbia residents who had received insured medical services while in New Brunswick. The information on that tape was being sent to British Columbia so that the New Brunswick Department could be reimbursed by the Ministry.

[13] The three other tapes contained the personal information of New Brunswick residents. The tapes had been shipped to New Brunswick previously from British Columbia and the information had been uploaded to the New Brunswick billing system. These tapes were being returned to British Columbia for re-use. The information of New Brunswick residents was a copy of the information contained in the records-keeping system of the Ministry here. Once the information had been received and processed by New Brunswick, British Columbia had no further need for it and the tapes could have been erased in New Brunswick before the tapes were shipped back to British Columbia. There was no policy or agreement in place between the New Brunswick Department and the Ministry to have the tapes erased before they were shipped back to British Columbia.

3.0 DISCUSSION

[14] Public bodies in British Columbia are statutorily required to take reasonable measures to protect personal information in their custody or under their control. Section 30 of FIPPA sets out the legal requirement:

> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[15] There are two issues in this investigation:

1. Did the Ministry have reasonable security measures in place to protect the personal information which it was sharing with other jurisdictions, as required by s. 30 of FIPPA?

2. Did the Ministry take reasonable steps in responding to the loss of the tapes?

[16] **3.1 Reasonable Security Measures**—Section 30 of FIPPA requires a public body to take all reasonable measures to protect personal information under its custody or control. In Investigation Report F06-01,[2] dealing with the provincial government's sale of computer backup tapes containing personal information, I said this about the meaning of "reasonable":

> [49] By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.
>
> [50] The reasonableness standard in s. 30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.

[17] The nature and level of security will depend on the sensitivity of the information. As was also noted in Investigation Report F06-01:

> [52] The sensitivity of the personal information at stake is a commonly cited, and important, consideration. For example, a computer disk or paper file containing the names of a local government's employees who are scheduled to attend a conference or take upcoming vacation does not call for the same protective measures as a disk containing the medical files of those employees.
>
> [53] Sensitivity is a function of the nature of the information, but other factors will also affect sensitivity. For example, the sensitivity of medical treatment information for someone who died 70 years ago is less than for someone who died more recently or is living.

[2] [2006] B.C.I.P.C.D. No. 7.

[18] **3.2 Analysis of Security Measures**—The personal information of British Columbia residents here did not consist of medical files or the results of medical tests. If someone had access to the medical billing codes, however, the tapes would convey information about treatment received by identifiable British Columbia residents. Further, the information could be used to cause financial or other harm to individuals.

[19] The fact that the tapes could, it appears, only be read by special computer equipment is not an answer in itself. Information security through technological obsolescence is not a best practice and, while it may be relevant under s. 30, it is not adequate in this case. In assessing this issue, moreover, I note that the Ministry's use of unencrypted tapes did not comply with the 2006 direction of the provincial government's Chief Information Officer to all provincial government ministries that "sensitive or personal information must be encrypted when stored on portable storage devices to ensure protection from loss, compromise or unauthorized disclosure."[3] By failing to encrypt the personal information being shared, the Ministry failed to meet its duty under s. 30.

[20] Another s. 30 consideration relates to the method of transferring the personal information. The use of a bonded courier service is, generally, considered to be a reliable method of transporting materials. As with other delivery methods, courier delivery is not infallible and a certain percentage of packages are misplaced or lost. Courier companies and Canada Post can provide shipment tracking mechanisms to track shipments along their journey and offer tracking services to help locate missing packages and assist in their recovery if they do go astray. These features of delivery services can be relevant in assessing the reasonableness of security measures respecting the shipment of personal information.

[21] In this case, the tapes were shipped from New Brunswick on October 3, 2007. There was no policy or agreement in place under which the agency shipping information would notify the recipient agency of the shipment or when to expect it. Nor did either agency have a policy in place requiring routine tracking of a shipment in order to help ensure its delivery. Because of this, no efforts were made to try to track the shipment of tapes from New Brunswick until October 25, 2007, over three weeks after they were shipped. It is reasonable to suggest that the sooner an item is known to be lost, the more likely it is that a search for it will succeed. It is reasonable to conclude that the delay in this case may well have contributed to the inability to find these tapes.

[22] Considering all of these factors, including the nature of the information involved, the failure to use encryption and the ease with which a tracking policy could have been adopted and implemented, I conclude that the Ministry did not comply with its s. 30 duty to take reasonable security measures to protect personal information against unauthorized disclosure or use.

---

[3] Chief Information Officer memorandum of June 2, 2006 to all Assistant Deputy Ministers, Corporate Services (reference 44692): http://www.cio.gov.bc.ca/rpts/memo/44692MemoCIOMemory.pdf. This direction is consistent with ISO27002:2005, the internationally-accepted standard for information security practices and with the provincial government's own information security policies.

[23] **3.3 Steps Taken Afterward**—In order to assist public bodies, the OIPC has published a key steps document for managing privacy breaches.[4] When a privacy breach occurs, public bodies and service providers need to make every reasonable effort to recover the personal information, minimize the harm resulting from the breach and prevent future breaches from occurring. The OIPC's key steps document has been useful in our review and evaluation of the Ministry's actions in this case. The four key steps public bodies must undertake in managing a privacy breach are:

1. Contain the breach;
2. Evaluate the risks;
3. Determine whether notification of affected individuals is required; and
4. Develop prevention strategies to reduce risks in the future.

[24] The first three steps should occur as soon as possible following the breach, either simultaneously or in quick succession.

Contain the breach

[25] On October 25, 2007, staff at the New Brunswick Department and HIBC both learned that the tapes had not arrived in British Columbia. The New Brunswick Department contacted the courier company, which initiated tracing procedures. Once the courier company advised that the package could not be found, the New Brunswick Department initiated an internal investigation. It also called the Richmond Detachment of the RCMP, which began a police investigation. X-Wave was directed to create a new tape of the British Columbia residents to replace the missing tape and to create a record of the New Brunswick residents whose personal information would have been on the missing tapes. These were appropriate steps to take in the circumstances.

[26] However, while the circumstances surrounding the loss of the tapes were still under investigation, the New Brunswick Department shipped a replacement tape to British Columbia using the same method which had resulted in the potential privacy breach. Although this personal information was under the control of the New Brunswick Department, there is no indication that HIBC objected to the shipping of the personal information of British Columbia residents using this unencrypted method. Fortunately, HIBC received the second shipment without mishap.

Evaluate the risks

[27] In order to determine what additional steps are immediately necessary, public bodies are expected to evaluate the risks associated with the breach. Some of the

[4] A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. Common privacy breaches involve theft or loss of personal information of customers, patients, clients or employees. Examples include when a computer containing personal information is stolen or personal information is mistakenly sent to the wrong person.

factors a public body should take into consideration when evaluating the risks associated with a breach are set out in Order P06-04:[5]

> [80] In discussing what "reasonable security arrangements" entail in Investigation Report F06-01, I considered the relevance of the sensitivity of the personal information at stake, the foreseeability of a privacy breach and resulting harm, the relevance of generally accepted or common practices in a particular sector of kind of activity, the medium and format of the record containing the personal information, the prospect of criminal activity or other intentional wrongdoing and the cost of security measures.

[28] In this case, the main risk identified by the Ministry was that of identity theft. The amount and type of personal information contained on the tapes would, certainly, be sufficient to begin the process of "social engineering", which could result in a third party obtaining additional information, identification documents or credit in the affected individual's name.

[29] On November 1, 2007, the MSP files of the affected individuals were flagged. Where an MSP file is flagged in this way, an individual cannot obtain insured health services without presenting an MSP CareCard and further documentation to confirm identity. This helps prevent medical services being obtained fraudulently and may assist in the apprehension of an individual using stolen identity information. But the flagging of MSP files is not a direct and proximate risk-reduction measure in relation to identity theft risks.

Determine whether notice is required

[30] Notification can be a key step in responding to a privacy breach, primarily notice to the affected individuals, but also to other groups in some cases. An important purpose of notification of affected individuals was described in Investigation Report F06-01:

> [106] …In my view, the key (but not sole) consideration overall should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been disclosed.

[31] In this light, for notification to be effective it must be given in a timely enough fashion to allow those affected to effectively mitigate the breach's risks. The reasonableness of the timing is measured by whether it is objectively prudent in all the circumstances.

[32] In this case, the Ministry decided that individual notification of the 124 affected individuals was appropriate. The notification letters included information about the flagging of their MSP files and the possible implications for the individual. They also advised, at the OIPC's suggestion, that the Ministry would pay the cost of obtaining

[5] [2006] B.C.I.P.C.D. No. 35.

credit reports, for having flags (alerts) placed on individual credit files, and costs flowing from having such a flag on one's credit report. The Ministry further offered to cover the costs of having a credit monitoring agency provide services to the affected individuals. These actions can be effective in mitigating the effects of any privacy breach.

[33] However, it took 41 days from the time that it was first known that the tapes were missing until the mailed notices went out to the affected individuals. This delay meant that mitigation strategies were almost certainly less effective than if they had been implemented as soon as the tape loss was discovered, which was already about three weeks after the tapes left New Brunswick.

[34] The Ministry also decided to notify the 570 physicians who had provided medical services to New Brunswick residents that their practitioner numbers had been involved in a potential privacy breach. These notifications did not occur until late December 2007.

[35] As pointed out in the OIPC's resources on privacy breaches, the OIPC ought to be notified where appropriate following a privacy breach, taking into considerations such factors as:

- the sensitivity of the personal information;
- whether the personal information could be used to commit identity theft;
- whether there is a reasonable chance of harm from the disclosure including non-pecuniary losses;
- the number of people affected by the breach, and
- whether the information was fully recovered without further disclosure.

[36] In this case, the Ministry became aware of the missing tapes on October 30, 2007, yet did not report the breach to the OIPC until December 10, 2007, even though the tapes containing the personal information remained unaccounted for. While FIPPA does not explicitly require that the OIPC be notified of privacy breaches, prompt notification to the OIPC aids the OIPC in assisting public bodies and affected individuals. In the case of public bodies, this may help them develop effective strategies to mitigate the risk of harm, or actual harm arising from a breach. The best practice, therefore, is to notify the OIPC promptly of a privacy breach, where appropriate after consideration of the factors listed above.

Develop prevention strategies

[37] To comply with FIPPA's security requirements, a public body should develop and implement breach prevention strategies. In this case, the breach was caused by sharing information in an unsecured format and in not erasing certain personal

information elements once they were no longer of use. As a result of this incident, the Ministry conducted a review of the following areas:

- sharing billing information with other jurisdictions,
- communication and reporting of privacy breaches.

[38] The Ministry also hired an independent security consultant to assist with a review of privacy processes related to this incident.

Sharing billing information with other jurisdictions

[39] As a result of this incident, on December 10, 2007, the Ministry asked HIBC to closely track any tapes already in transit to or from other jurisdictions. Effective December 11, 2007, the Ministry stopped transferring unencrypted information to other jurisdictions. On December 17, 2007, the Ministry directed other provinces and territories to cease transferring unencrypted personal health information to British Columbia. The Ministry also asked provinces and territories to destroy any unencrypted magnetic tapes in their possession which had originated in British Columbia and to provide certificates of destruction. Encrypted CDs containing information which originate in British Columbia are to be destroyed after they have been processed and a record is maintained of the destruction.

[40] At the time of this incident, the Ministry was working with New Brunswick to replace the magnetic tape technology with encrypted CDs. The Ministry was already using encrypted CDs for sharing billing information with Saskatchewan. After the loss of the tapes, as an interim measure, the Ministry and New Brunswick started using encrypted CDs for information exchanges. Manitoba, Alberta, Ontario and Newfoundland are also now exchanging data with British Columbia using encrypted CDs.

[41] Beyond the transfer of reciprocal billing information with provincial and territorial health ministries, the Ministry has told the OIPC that it is working to converting other paper-based transfers, such as MSP group billings to large employers, to encrypted and password-protected CDs.

[42] The Ministry also told the OIPC that its objective is to move away from the transfer of physical media containing personal information to the use of a secure electronic FTP process. The Ministry raised this suggestion at a meeting of the Inter-provincial Working Group on Hospital and Health Care Insurance in November 2007. On February 12, 2008, the Ministry sent a letter to other provinces and territories offering a web-based Secure File Delivery Service (SFDS) to exchange reciprocal billing information. As of the date of this report, Nunavut, Manitoba and a Federal group have agreed to use the SFDS, and are preparing to do so. Other secure information transfer processes, including encrypted CDs, will continue to be accepted by British Columbia as long as they meet the security standards that British Columbia has established for personal information sharing.

Communication and reporting of privacy breaches

[43] The Ministry has told the OIPC that it has strengthened the monitoring process for exchanging reciprocal billing data. It now requires the receiver to be notified of impending shipments and to confirm receipt upon arrival. Courier services transporting encrypted CDs must provide up-to-the-minute tracking information and must obtain a signature confirming delivery.

4.0 CONCLUSION

[44] In summary, the OIPC's findings are that:

1. In the circumstances of this case, reasonable security required that the information be secured using encryption. Since encryption was not used on magnetic tapes, the use of such a medium for the inter-provincial sharing of this type of personal information did not meet the standard required by s. 30 FIPPA.

2. The steps taken by the Ministry to mitigate the potential damage from the privacy breach included:

   - placing a flag on each person's Medical Services Plan file to alert a service provider in cases where PHN card could not be produced;
   - halting the sharing of unencrypted personal information with other jurisdictions;
   - notifying the affected British Columbia residents of the potential privacy breach to alert them to the possibility of misuse of their personal information;
   - notifying the medical services providers that their practitioner numbers may be subject to misuse;
   - offering to pay for credit reports and credit monitoring services for affected individuals to help them take appropriate mitigation steps on their own to reduce the impact of the information loss.

   Considering the sensitivity of the personal information involved and lack of security afforded by the magnetic tapes, the decision to notify affected individuals was appropriate in this case. However, the purpose of notification is to afford the affected individuals the opportunity to take steps to mitigate the harm that might result from the possible privacy breach. The effectiveness of these mitigation measures diminishes over time. By delaying notification of individuals for over five weeks, the Ministry failed to meet its obligations under s. 30 of FIPPA.

3. The actions taken by the Ministry to prevent a recurrence of this privacy breach are these:

- eliminating unnecessary transfers of personal information;
- ensuring that the transfer of personal information with other provinces and territories only occurs using encryption protected media;
- strengthening the tracking and monitoring practices for any physical data transfers that are made;
- working towards the elimination of unsecured media transfers of personal information with other government sectors and large organizations;
- offering electronic secure file delivery services to other provinces and territories for the exchange of reciprocal billing information; and
- developing long-term plans for secure and sustainable electronic data transfers over the internet.

These efforts by the Ministry demonstrate an understanding of its responsibilities under FIPPA to protect personal information and a willingness to make appropriate changes to ensure that a similar incident does not occur in the future.

[45] I make no further recommendations in this matter.

[46] The Ministry co-operated fully with our investigation and that co-operation is appreciated.

[47] Wayne Zimmerman, Portfolio Officer, conducted this investigation and prepared this report. Jim Burrows, Portfolio Officer, assisted with completion of this report.

May 7, 2008

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

OIPC File: F07-33520