NBPPIA-2008-01

INVESTIGATION INTO LOST PERSONAL INFORMATION BY THE DEPARTMENT OF HEALTH – MEDICARE BILLING CARTRIDGES

April 2008

1.0 Introduction

New Brunswickers cherish their privacy. Like most Canadians, New Brunswickers consider personal health information to be among the most sensitive information they own. They have a very high expectation of privacy in respect of this information and want it to be jealously protected.

The medical profession and all the healing arts are founded upon a relationship of trust which starts with a healthy respect for patient privacy. The law also respects the high standard of care which must be exercised when dealing with personal information, such as health information, since it may reveal intimate secrets about a person's history or condition and often sits very close to the biographical core of their being. As the mounting pressures for efficiencies in the health care sector and new technologies enable the development of electronic health records, New Brunswickers will face many new risks and threats to their privacy and the protection of their personal health information. For this reason the province is considering the adoption of a new legislative framework to ensure that patient confidentiality will be maintained and hopefully strengthened.

It is therefore regrettable that it is in this very context that we have had to investigate an easily avoidable privacy breach in the Department of Health. Most reported privacy breaches in Canada occur through some unintentional error. In this case the shipping company lost some Medicare billing tapes while in transit. The investigation has not revealed any evidence of malice or wrongdoing and the loss, while it remains unexplained, appears to have been inadvertent. The real story however is why was the information being transferred in this manner to begin with, and, more troubling still, why did it take so long for the loss to come to light and to be addressed? Our investigation has revealed that despite the Department of Health's much heralded promise of protecting patient privacy, there seems to have been a lack of commitment to privacy in the Department's head office leading up to this breach.

Policy development in this area was woefully lacking. There was no centre of responsibility to assist the Deputy Minister in meeting his accountability duties under the *Protection of Personal Information Act (POPIA)*. Front line staff and middle managers had no appreciation for the fact that even a mail handler, who never opens a package and has no access to personal health records, has obligations under POPIA and critical responsibilities in maintaining safeguards so that doctor/ patient, or nurse/ patient confidentiality is adequately protected.

In this context, when the story eventually broke, the hyperbole and hysteria spoke as tellingly about the confusion and lack of knowledge over how to proceed, as did the underlying lack of preparedness and dearth of adequate policies and safeguards. There were calls for the Minister's resignation daily, which invariably followed upon the Minister's daily updates on the situation in the Legislature. Everyone joined in the blame

game. Was it NB Medicare that was at fault or BC Health? Was there a problem throughout the system, or human error for which only a few should account?

This investigation has revealed that in fact there is no merit in apportioning any blame in this context to the courier company or to individual employees. In all instances these individuals were found to be carrying on their duties in accordance with existing policy and long established practice. What was lacking were adequate policies and safeguards to put in place the culture of privacy which POPIA's ten principles are meant to infuse into our public administration.

The following few pages will set forth in greater detail the background to this complaint, our investigative findings and some early recommendations that the Department should implement in a timely manner to raise the bar and insist on more rigour from all its employees in meeting their obligations under POPIA and in anticipation of more onerous obligations which will follow under a new personal health information protection law.

2.0 Background

Medicare is a billing system. When New Brunswickers, with a valid Medicare card, access services, physicians and other health care professionals provide the billing information to the Department of Health in order to be paid for the service provided. When a New Brunswick resident receives services in other provinces, those provinces look to the Province of New Brunswick to reimburse them for the cost of those services. The Province of New Brunswick has signed agreements (Interjurisdictional reciprocal billing agreements) with all other Provinces and Territories (other than Quebec) for recouping these costs. The provinces and territories exchange information with each other regarding the services that have been provided to out of province residents on a scheduled basis. This exchange may occur more or less frequently depending on the volume of the information.

The information that is exchanged between the provinces includes the patient's name, Medicare number, date of birth and gender along with billing codes. Each province has an agreement with the government of New Brunswick regarding exchanging the information. At the time of this investigation Alberta, Manitoba, Newfoundland, Ontario and PEI sent the information via encrypted CD. Yukon, Nunavut and the Northwest Territories sent the information in paper form. Up until December of 2007, British Columbia sent it by cartridge. New Brunswick and Nova Scotia share the information using FTP (Short for File Transfer Protocol, the protocol for exchanging files over the Internet).

Prior to December of 2007, the process for sending the information to British Columbia was as follows. BC creates the cartridge that contains the list of services NB residents received while they were in BC. The unencrypted tape is sent to the NB data center (which is the responsibility of the Department of Supply and Services) where the Medicare database is located. The data center, which is run by an independent contractor,

notifies the Medicare Operations Branch that the tape has arrived. The cartridges are sent to the tape librarian where it is held for processing. The tape would be executed during the monthly billing run. Once the tape is processed, it is sent back to the tape library where it is packaged by the tape librarian and sent back to BC with any cartridges that may contain the same information of BC residents who received services in New Brunswick for which the New Brunswick government is looking for reimbursement.

On October 3, 2007 a contractor of the New Brunswick Department of Supply and Services sent 4 cartridges containing patient information and billing information to Health Insurance BC (HIBC) using a courier company. On October 25, 2007 DOH was notified by HIBC that the package had not arrived and asked for the name of the courier company. HIBC contacted the courier company to inquire as to the location of the package. The courier company informed HIBC that the package was missing. The cartridges contained Medicare billing information pertaining to 485 New Brunswick residents and 149 British Columbia residents. On October 26th, DOH staff requested that the contractor create another cartridge. The recreated cartridge was sent to HIBC on October 31, 2007 and arrived safely.

It wasn't until November 29th that senior officials in the department became aware that the cartridges containing the personal information were missing through an email on a related topic. The senior official in question was out of the province at the time and initiated an internal investigation into the missing cartridges.

On December 10th, 2007 the Office of the Ombudsman was notified by the British Columbia Information and Privacy Commissioner's Office that the cartridges had gone missing. The Office of the Ombudsman contacted the Department of Health and proceeded to investigate the breach.

In addition to investigating the lost cartridges, the Minister of Health asked my Office to undertake a review of the adequacy of the policies and practices surrounding the collection, use and disclosure of personal information by the Department of Health. I commend that Minister for identifying the need for a review. After reviewing his request, I informed the Minister that given the large volume of resource intensive work required and the need for our Office to remain independent it would be more appropriate for the Department to hire external resources to perform the review. I offered the assistance of my Office to 1) help his officials draft the Request for Proposal for such resources, 2) receive and comment on progress reports, 3) review and comment on recommendations received and 4) provide oversight during implementation.

I will reserve comment on the larger review to the appropriate time and limit this report to the privacy issues arising from this particular breach.

3.0 Analysis

3.1 The Law

Section 2(1) of the *Protection of Personal Information Act* makes every public body subject to the Statutory Code of Practice which is contained in Schedule A of the *Act* and interpreted in accordance with Schedule B. The Department of Health (DOH) is one of those bodies to whom the Act applies. The Statutory Code of Practice is based on the ten privacy principles developed by the Canadian Standards Association; (1) accountability, (2) identifying purpose, (3) consent, (4) limiting collection, (5) limiting use, disclosure and retention, (6) accuracy, (7) safeguards, (8) openness, (9) individual access and (10) challenging compliance. The two of particular concern in this situation are Principle 1: Accountability and Principle 7: Safeguards.

Principle 1 in Schedule A provides that 'A public body is responsible for personal information under its control. The chief executive officer of a public body, and his or her designates, are accountable for the public body's compliance with the following principles.' There was no privacy policy at the Department of Health designating anyone as responsible for compliance with the privacy principles; therefore this role falls to the Deputy Minister as the chief executive officer.

Principle 7 in Schedule A provides that 'personal information shall be protected by safeguards appropriate to the sensitivity of the information'. Schedule B further elaborates by stating that 'the safeguards to be adopted include training and administrative, technical, physical and other measures, as appropriate in the circumstances, and include safeguards that are to be adopted when a public body discloses personal information to a third party or makes arrangements for a third party to collect personal information on its behalf.'

3.2 Severity of the Breach

The information in question was sent by cartridge. The information on the cartridge included the patient name, Medicare number, date of birth, gender, service date, service code (numeric code), diagnostic code (numeric code), practitioner number, and speciality code. In order to understand what service was provided by the practitioner, you would need to have access to the list of codes with their explanations.

According to the IT branch at DOH in order to read the cartridges a special drive, drive controller, mainframe or midframe and software are required. As indicated by DOH this technology was only mainstream in data centers and has been retired from most of them. While the information was not encrypted or password protected like the CD's sent between other provincial governments, obsolete technology would be required in order for anyone to access the information available on the cartridge. It is unlikely that a third party could have accessed the information contained in the cartridges.

The courier company has informed the contractor that the package is lost. The RCMP have visited the last terminal in which the cartridge was scanned in and believes that the package was lost and not stolen.

When analyzing the severity of the breach, it is important to note that the cartridges are believed to be lost. Additionally, while they do contain personal information the health information is limited to billing information which is not as sensitive as diagnostic or detailed health information. In order to access the information on the cartridge, a mainframe computer and relatively obsolete technology is required.

The concern however is that if the information could be accessed, the cartridges do contain name, gender and Medicare number which would assist anyone interested in using the information for identity theft. Identity theft occurs whenever someone uses personally identifying information, like one's name, social insurance number, Medicare number, or credit card number, without permission, to commit fraud or other crimes. According to the Privacy Commissioner of Canada total losses from identity theft worldwide are in the billions of dollars, making identity theft "the crime of the 21st century". With this information, criminals can obtain credit cards in the victim's name that they max out and don't pay leaving the victim with a poor credit rating and an unpaid bill. They can also try to open up a bank account or take out a mortgage depending on the amount of personal information available to them.

3.3 Security Measures in place before the incident

The security measures in place at the time of the incident revolved around the physical security of the data center itself and did not include the process of transmitting the information. The data centre that houses the mainframes on which the information resides is at a lockdown location only accessible by authorized personnel. Additionally security features such as security cameras positioned throughout the center and surrounding area are in place.

After the cartridge leaves the data center, the attention to security seems to reduce. The cartridges are placed in regular envelopes. They are sent via courier with both the addressee and the addressor indicated. There was no tracking system in place through either the courier company or through the Departments that would indicate that a package arrived on time. Additionally tamper proof tape was not used.

As outlined above the interpretive guidelines applicable to POPIA's Principle 7 state specifically that the standards required "include safeguards that are to be adopted when a public body discloses personal information to a third party". The contracts which the Department of Supply and Services had with its supplier X-wave were inadequate in terms of the contractual guarantees that would be appropriate having regard to the sensitive nature of the information transacted through the Medicare billing information system. Our review has not included any review of the security architecture of the Medicare Billing system itself, which we understand is a legacy system.

3.4 Policies and Procedures of the Department

In September of 2007, the New Brunswick Government approved the Government Information Technology and Security Policy (GISSP). In the standards & directives document for the policy it states that:

> *Government information is a valuable asset…To ensure that the information can continue to be used for the purposes for which it is collected, it must be protected from unauthorized disclosure, modification, use or destruction – steps must be taken to ensure its ongoing confidentiality, availability and integrity.*

The standards and directives are based on best practices and industry standards. They provide standards for passwords, provision of access, workstation security, email security, etc. The document does not address the transfer of that information outside of the province.

At the time of the breach there was, at DOH, no protection of personal information policy, no policy to address how this information should be sent and no privacy breach policy. One official within the department admitted to our investigators that this was not the first time that Medicare billing tapes had gone missing in this manner. According to this account, when the department was informed by BC Health that the tapes had not arrived, the only response as per established practice, was that new tapes were made of the same billing information and sent off in the same manner. The organizational culture made it quite clear that bills must be paid. Unfortunately, protecting patient confidentiality did not benefit from the same zealous enforcement**.**

3.5 DOH's Response to the Breach

After senior officials in the Department were made aware of the breach, several actions were taken. DOH stopped sending the information by cartridge and worked with HI BC to devise protocols to send the information by encrypted CD in the short term. Prior to the breach, the two organizations had been working for several months on changing the process from cartridges to encrypted CD. Unfortunately, this process was not completed prior to the cartridges being lost. The Department has expedited talks with other jurisdictions to move to file transfer protocol (FTP) for transmitting this type of information.

In addition to working towards finding a more secure way to transfer the information, the Department also focused on notifying the affected parties. The Minister provided public notice of the breach in the Legislative Assembly on December 11, 2007. On the same day DOH began to contact the affected individuals by phone. The department sent out letters to the individuals they could not reach by phone on December 14, 2007. Advertisements were placed in New Brunswick and British Columbia newspapers. The Department offered all of the affected parties credit monitoring services for an entire year.

The breach also alerted the department to the lack of policies in place to handle this situation. After the breach, a Data Breach policy was developed. The department began a

review of the risks relating to all transfers of Medicare data. Additionally, a secure data transfer analysis was conducted in December in order to determine a more secure process for transferring data between jurisdictions. A memorandum was sent to all staff of DOH informing them that any breach of personal information was to be reported to the Deputy Minister.

3.6 Findings

Protective Measures - The measures in place at the time of the breach were not sufficient given the sensitivity of the personal information. The information was being transferred in an insecure format. Several recent decisions by privacy Commissioners in Canada have confirmed that any time personal health information leaves the confines of the physical establishment where it is kept, whether on a laptop, blackberry, CD or other portable device, the information must be encrypted. The better safeguard is to develop policies and practices which minimize the use of such information outside of health care facilities. The Department of Health has a leadership role in ensuring that the Regional Health Authorities and all custodians of personal health information adopt and enforce such minimal safeguards. In this context, I find the Department's failure to move more expeditiously in adopting FTP methods and encrypted CD technologies as provincial standards for the transfer of medicare reciprocal billing information, in all instances to be a failure to meet their obligations under principle 7 of the *Protection of Personal Information Act.*

After the breach, the Department researched the best practices for transferring physical data including those of other government departments, the RCMP and the Treasury Board of Canada. They have indicated to our Office that they will be implementing these measures including using tamper proof tape and a system for tracking the documentation. Additionally, both before and after the breach, the department has been working with other health departments through the inter-jurisdictional working group to establish more secure manners of transferring the data. In my view, these responses are encouraging, but insufficient.

As a bare minimum the Department failed to take adequate safeguards in keeping with its obligations under POPIA by failing to erase the sensitive information of the 485 New Brunswick residents before sending the tapes back to BC with the additional reciprocal billing information of the 149 BC residents who had received services here. HIBC had no further use for the New Brunswick information and the failure to remove the sensitive information from these tapes before sending them back in the mail was negligent.

Policy Documents - Policy documentation on protection of personal information and breach notification was severely lacking. The Department of Health deals with personal information and personal health information on a daily basis. Our investigation revealed a lack of policy documents that address the importance of protecting personal information. It also indicated a lack of understanding by staff of the importance of protecting personal information. Given the amount of personal information in the hands of the department as

well as the development of electronic health records, it is important that the Department of Health does a better job at protecting that personal information.

Breach Notification - It took over six weeks for senior officials at the Department of Health to become aware of the missing information. This is not the fault of any one individual, but a result of a lack of policy and procedures within the organization. After the breach, an internal memorandum was sent to all staff within the Department of Health indicating that any breach or suspected breach of personal information, such as a stolen laptop or packages lost in the mail, is to be reported immediately to the Deputy Minister. While this is a commendable start, it simply does not go far enough.

Training - The Minister stated in his address to the Legislature that the Department gives "the protection of personal patient information our highest priority. We know that New Brunswickers have entrusted us with this information and we have a duty to maintain this trust." Once senior members of the Department became aware of the lost tapes, they acted quickly to investigate the breach and notify the affected parties. I have no doubt that the Minister and senior officials are painfully aware of the importance of protecting personal information. Given the fact that no one was made aware of the lost cartridges until nearly one month after it went missing, I am not certain that all employees within the Department are as aware of the importance of protecting personal information.

4.0 Recommendations

(1) Accountability – It is recommend that a Chief Privacy Officer position be created for the Department of Health.

The Department of Health needs a Chief Privacy Officer (CPO) similar to the Corporate Privacy Officer at Service New Brunswick. This individual should be a senior executive. The role of the privacy officer would be to develop a department wide privacy philosophy that would include the development of policies, practices and protocols; training of staff, assisting in the creation of data flow maps, reviewing Privacy Impact Assessments (an analysis of projects in order to identify their privacy risks), reviewing or creating retention schedules, updating policies, practices and protocols after the introduction of any new legislation and performing internal privacy audits.

By creating this position and giving it internal legitimacy, the Department would be going a long way towards satisfying their accountability responsibility under Principle 1 of the *Protection of Personal Information Act*. The Chief Privacy Officer could assist the Deputy Minister in fulfilling his role as the statutorily designated person accountable for the public body's compliance with the privacy principles. They could also be the liaison between the Department and the Regional Health Authorities. This would assist with the development of consistent privacy policies and practices between the organizations.

(2) Policy & Procedures – It is recommended that the Department of Health create a comprehensive privacy policy and incorporate this policy into individual procedures. This policy should be reviewed on an annual basis.

The Department of Health needs a comprehensive privacy policy for the organization. Prior to developing this policy, the Chief Privacy Officer recommended above would need to examine the current information handling practices and develop a data flow map to determine how information flows within and outside of the organization. After the development of a department wide privacy policy the CPO would then need to drill down to individual and team positions to ensure that the procedures for these individuals and teams incorporate privacy, in particular the detecting and reporting of privacy breaches.

The privacy policy should include references to the Department of Health's obligation under POPIA and any future legislation and definitions of personal information and personal health information, privacy breaches, etc. It should identify accountability points, address employee privacy issues and contract clauses, to name but a few points.

(3) Training – It is recommended that the Department of Health provide additional training to employees on POPIA.

The Office of Human Resources, through an independent contractor, has developed an online course on the *Protection of Personal Information Act*. This course is made available to employees through the Knowledge Centre, an intranet site used for facilitating on-line learning. The Department of Health should implement a procedure to track which employees have received the training to ensure that all current and new employees have taken the course. Additionally, the Department should include in their training follow-up with employees as to how protecting personal information is applicable to their particular position.

(4) Notification – It is recommended that draft health information privacy legislation include a requirement to notify the Office of the Ombudsman of beaches.

One of the recommendations of the New Brunswick Task Force on Personal Health Information released in September of 2007 was that 'when a data custodian breaches an obligation or whenever a privacy safeguard fails, the data custodian, in addition to notifying the individual(s) affected by the breach or failure, also be required to notify the Information and Privacy Commissioner'. It this particular case, the Department did notify the individuals affected by the breach. However, the Office of the Ombudsman was made aware of the situation by the Information and Privacy Commissioner of British Columbia. It would be more appropriate in the future for the custodian to notify the Office of the Ombudsman directly. I wholeheartedly support the Task Force's recommendation that custodians provide notice to the oversight body.

In this case, while our call to the Department of Health got ahead of any formal notification to our office, the Department of Health made every effort to keep us up to

date on its actions and progress in response to the breach incident and has been extremely helpful during this investigation.

(5) Contracting out – It is recommended that the Department of Health conduct a review of all existing agreements with information management suppliers and other vendors involved in the collection, treatment or use of personal health information to ensure that adequate contractual safeguards are in place

Not only in the current context, but increasingly as government moves ahead with the delivery of infoway applications in this province, the Department of Health will be dealing on an interim and long term basis with private sector solution providers who will have access to personal health data stored electronically, for the purpose of system development and maintenance. It is critical that such uses be minimized and that adequate safeguards be taken in the development and piloting of these initiatives to not place any greater risk to personal health information than is strictly necessary. In the long term, system maintenance work that is contracted out, as was the case here, must be subject to legal obligations and provisions that are consistent with best privacy practices in the field.

(6) Next Steps – The Department of Health must move ahead quickly with the full review of its information management practices with the assistance of outside expert counsel.

As outlined above, our office was invited but has declined the Minister's invitation to carry out an in-depth review of all the information management practices in the department of health, to verify and improve their privacy and security. While, for the reasons set out above, it is not possible for the Ombudsman to undertake a review of this scope and nature, it is obvious from our current investigation that such a system overhaul is urgently needed. It is critical, in my view, that this work take place as much as possible before further infoway projects are rolled out. Before proceeding with any further development of the electronic health record, we recommend that all information support systems within the department be subjected to rigorous external threat risk assessments and privacy impact assessments.

By way of example, the department and experts they retain should look to the recent report of the Ontario Information and Privacy Commissioner in response to her review of privacy and security within the Ontario Agency mandated to assist with the automation of health informatics systems in health authorities across Ontario, the Smart Systems for Health (SSHA) review. That report contains 82 recommendations which SSHA has now largely implemented. The report and the response it received gives an interesting example of the work ahead in New Brunswick.

I will be pleased to return to this matter as the province finalizes the RFP and the terms of reference in respect of the review which the Minister earlier requested of this Office.

5.0 Conclusion

The breach of personal information that occurred in October of 2007 has hopefully served as a significant, if not painful, wake up call to the Department of Health as well as all other government departments: privacy is an issue that needs our full attention. It is not enough to say that protecting personal information is important within the organization. The Department of Health, as well as all other government departments, needs to insure that protecting personal information is a goal of every employee of the organization that handles personal information.

This investigation has helped make clear what several commentators have been saying for years. While the adoption of POPIA as New Brunswick's first public sector privacy law has helped raise awareness and has heightened the public expectation of privacy in their dealings with public authorities, it has had too little impact on the way public authorities manage personal information. The reasons for this may be varied, perhaps the law was not sufficiently prescriptive, or was too vague, perhaps too little was done in the area of employee training, perhaps insufficient resources have been allocated to properly administer the law, perhaps accountability has not been worked into the day to day responsibility of managers and staff or been appropriately considered in their performance evaluations. In many ways we have not yet seized upon how onerous a task it is to protect personal information in the age of e-government and on-line service delivery.

With a new legislative framework and with specific provisions in the health care sector, we will have a new opportunity to do the job right. Other provinces are doing so and are much further ahead of this curve than we are. It's time for New Brunswick to catch up to the rest of Canada.