OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

P-2010-001

March 29, 2010

Workplace Health, Safety and Compensation Commission

Summary:

In late January 2008, computer records containing the personal information of clients of the Workplace Health, Safety and Compensation Commission (the "WHSCC"), including health information, were exposed over the Internet by an employee of a health care services provider as a result of installing a popular music-sharing program, Limewire, on a laptop that also contained client files. The service provider was under contract to the WHSCC.

Upon request by the WHSCC our Office agreed to investigate and make recommendations with respect to the WHSCC's policies, procedures and security practices, and in particular measures that might be taken to further enhance the protection of WHSCC data in the hands of external contractors.

During the first phase of the investigation it became evident that the WHSCC had taken the appropriate measures immediately following notification of the breach to contain it, recover possession of the records and to determine the extent of the exposure. The WHSCC had also evaluated the risks of harm to affected individuals resulting from the breach, and had notified all of them within two weeks following the event.

During the second phase of our investigation our Office conducted a more in-depth review of WHSCC's information privacy and data security policies and procedures, and of the initiatives taken to enhance security following the breach. In particular our Office reviewed the terms and conditions governing information security, privacy and confidentiality in the contracts under which external health care service providers work, with a view to recommending steps to strengthen those provisions and their enforcement.

The Commissioner concluded that the WHSCC, prior to the breach, had made reasonable security arrangements within the meaning of section 36 of the *Access to Information and Protection of Privacy Act* (the *"ATIPPA"*) to protect the personal information of its clients against foreseeable risks. The Commissioner also concluded that following the breach, the WHSCC has taken reasonable measures to review the causes of the breach and to strengthen its policies, procedures and practices so as to minimize the risk of similar incidents in future. The Commissioner recommended that the WHSCC consider whether it would be reasonable to conduct a compliance audit of its contractual service

providers, and whether it would be reasonable to set a standard for privacy training for the employees of contractors, and to assist in the provision of that training.

Statutes Cited:

Access to Information and Protection of Privacy Act, SNL 2002, c. A1.1, as amended, sections 2(o), 7, 36, 39, 40, 51, 52; *Personal Information Protection and Electronic Documents Act,* SC 2000, c. 5; *Personal Health Information Act,* SNL 2008 c. P-7.01; *Workplace Health, Safety and Compensation Act,* RSNL 1990, c. W-11, as amended.

Authorities Cited:

Newfoundland and Labrador OIPC Reports P-2008-001; P-2008-002.

Other Resources Cited:

Key Steps When Responding to a Privacy Breach, Access to Information and Protection of Privacy Coordinating Office, Department of Justice, 2008; *Model Code for the Protection of Personal Information,* Canadian Standards Association, 1996.

I BACKGROUND

(a) The Workplace Health, Safety and Compensation Commission

[1] The Workplace Health, Safety and Compensation Commission ("WHSCC" or "the Commission") of Newfoundland and Labrador is a government agency that promotes safe and healthy workplaces, and provides return to work programs and compensation to workers injured in workplace accidents through an employer-funded, no-fault liability insurance plan under the provincial *Workplace Health, Safety and Compensation Act* (the "*WHSC Act*"). Reporting to the Minister of Human Resources, Labour and Employment, WHSCC has over 390 employees working out of offices in St. John's, Grand Falls-Windsor and Corner Brook.

[2] Over 16,000 employers operating in Newfoundland and Labrador are registered with WHSCC, and at any given time the Commission has active files dealing with approximately 12,000 injured workers. There are between 7,000 and 8,000 new claims each year. Some of the many services needed by injured workers are provided directly by the Commission, but many more are provided by outside health care providers including physicians, physiotherapists and occupational rehabilitation providers. In those cases, the costs of health care services are covered by the Commission, but those services are provided by private clinics under contract with WHSCC.

[3] Injury or illness claim files can range from relatively simple first aid incidents to those involving complex medical treatment and lengthy rehabilitation programs. Naturally, both the Commission and the health care providers involved in these programs must necessarily collect a great deal of personal information from individual clients. This may include basic identifying information such as name, address and other contact information, sex, date of birth and provincial Medical Care Plan ("MCP") number, as well as medical information, including details of illness or injury, testing, diagnostic and treatment information, employment history, rehabilitation and training program participation, and more.

(b) The "Incident"

[4] On January 22, 2008, an employee of a computer security firm in New York contacted the government of Newfoundland and Labrador to advise that he had discovered, on the internet, a significant amount of personal medical information and occupational rehabilitation information.

This information consisted of records that appeared to have been prepared by an occupational rehabilitation centre in this province in the course of performing evaluations for WHSCC as well as for other clients.

[5] The warning was passed on to WHSCC and the Department of Health and Community Services, and an investigation was begun immediately. By the afternoon of January 23, 2008 it was determined that neither the WHSCC's nor the Department's data systems had been compromised. It was determined that the source of the information in question was a laptop computer owned by a private rehabilitation services provider and used by one of that company's employees in the field.

[6] The breach had happened in the following way. The employee had collected a great deal of personal health information from clients in the course of her work, and those files were kept on the laptop, which she carried with her at work appointments and also took home. Around the end of December, 2007, the employee installed a program called "Limewire" on the laptop. Limewire is a popular peer-to-peer file-sharing program that enables individuals to exchange digital music files by downloading them from each other's computers via the internet. However, when the employee installed the program on her laptop, she unwittingly gave it access, not only to her music files, but also to all of the other files on the laptop as well. Therefore, on the several occasions between December 30, 2007 and January 22, 2008 that the employee logged in to Limewire to download music files, and also on every other occasion on which she was connected to the internet, Limewire was running and exposing all of the files on her computer over the internet.

[7] The employee's personal information, including her telephone number, was on the laptop and was exposed on the internet along with the other files. On the afternoon of January 22, 2008 the security company that had discovered the breach contacted the employee directly by telephone and advised her of what had happened. On their advice she disabled the Limewire program at that time. The next day, she brought the laptop to her employer's St. John's office. That same day her employer in turn brought the computer to WHSCC, where it was packaged and sent by courier to Electronic Warfare Associates ("EWA") of Ottawa, for forensic analysis.

[8] EWA found that between December 30, 2007 and January 22, 2008 there were a total of over 3,000 files, of all kinds, on the laptop's hard drive, that were being shared over the internet by the

Limewire program. Most of those were either music files, or other types of files that contained no personal or otherwise sensitive information. There were however 694 files that contained information that could be considered sensitive, and which *could* have been downloaded by another Limewire user. The Limewire program, however, does not keep a detailed log identifying which files have been downloaded or uploaded, so it is not possible to be certain how many files containing personal information had actually been viewed by anyone other than the security company that initially discovered the breach.

[9] On review of the laptop files, WHSCC confirmed that they contained the names, family status, work history, detailed physical assessments, and other information such as medications, allergies and mental capacity issues, of 155 individuals, of whom 108 were clients of the Commission. Of those, 21 files included dates of birth. None of the WHSCC files contained MCP numbers, which have individual birth dates embedded in them. Most did contain WHSCC file numbers, but those are sequential file numbers used only by the Commission. There were, in addition, three other files containing information belonging to other government employees, and files of 44 other individuals who were other clients of the private rehabilitation company.

[10] On January 24, 2008, the day after it was informed of the breach, WHSCC notified this Office of the occurrence. Following some informal contacts, the Commission wrote on February 26, 2008 to formally request that our Office conduct an investigation into the circumstances surrounding the privacy breach, and the Commission's policies, procedures, security practices and response to the incident.

[11] Our investigation was done in two stages. In the first stage, an investigator from this Office was assigned and over the course of several months, with the assistance of WHSCC personnel, assembled the documentation and other information relevant to the privacy breach and the immediate response to the breach by the Commission. The second phase involved a more in-depth review of information privacy and data security policies and procedures, and updates on changes made by the Commission to enhance security following the breach.

[12] Part of the request letter reads as follows:

> *We understand that your jurisdiction may be limited in this case, as the action which resulted in the information exposure was the responsibility of a private company and thereby falling under federal legislation and the jurisdiction of the Privacy Commissioner for Canada. Nevertheless we do request that you conduct an investigation of this incident concerning the Commission's policies and procedures with respect to security practices and the protection of privacy by external service providers.*

I will comment on the question of jurisdiction and responsibility at an appropriate juncture in the course of this report.

II STEPS IN RESPONDING TO A PRIVACY BREACH

[13] Section 36 of the *Access to Information and Protection of Privacy Act* (the "*ATIPPA*") states as follows:

> *36. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

[14] Under the *ATIPPA,* personal information in the custody or control of a public body may only be disclosed in the specific circumstances set out in section 39 of the *Act,* which reads:

> *39. (1) A public body may disclose personal information only*
>
> *(a) in accordance with Parts II and III;*
>
> *(b) where the individual the information is about has identified the information and consented to the disclosure in the manner set by the minister responsible for this Act;*
>
> *(c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose as described in section 40;*
>
> *(d) for the purpose of complying with an Act or regulation of, or with a treaty, arrangement or agreement made under an Act or regulation of the province or Canada;*
>
> *(e) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information;*
>
> *(f) to an officer or employee of the public body or to a minister, where the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister;*
>
> *(g) to the Attorney General for use in civil proceedings involving the government;*

(h) for the purpose of enforcing a legal right the government of the province or a public body has against a person;

(i) for the purpose of

(i) collecting a debt or fine owing by the individual the information is about to the government of the province or to a public body, or

(ii) making a payment owing by the government of the province or by a public body to the individual the information is about;

(j) to the Auditor General or another person or body prescribed in the regulations for audit purposes;

(k) to a member of the House of Assembly who has been requested by the individual the information is about to assist in resolving a problem;

(l) to a representative of a bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry;

(m) to the Provincial Archives of Newfoundland and Labrador, or the archives of a public body, for archival purposes;

(n) to a public body or a law enforcement agency in Canada to assist in an investigation

(i) undertaken with a view to a law enforcement proceeding, or

(ii) from which a law enforcement proceeding is likely to result;

(o) where the public body is a law enforcement agency and the information is disclosed

(i) to another law enforcement agency in Canada, or

(ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;

(p) where the head of the public body determines that compelling circumstances exist that affect a person's health or safety and where notice of disclosure is mailed to the last known address of the individual the information is about;

(q) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted;

(r) in accordance with an Act of the province or Canada that authorizes or requires the disclosure; or

(s) in accordance with sections 41 and 42.

> *(2) The disclosure of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.*

[15] The *ATIPPA* defines personal information in section 2(o) as follows:

> *(o) "personal information" means recorded information about an identifiable individual, including*
>
> *(i) the individual's name, address or telephone number,*
>
> *(ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,*
>
> *(iii) the individual's age, sex, sexual orientation, marital status or family status,*
>
> *(iv) an identifying number, symbol or other particular assigned to the individual,*
>
> *(v) the individual's fingerprints, blood type or inheritable characteristics,*
>
> *(vi) information about the individual's health care status or history, including a physical or mental disability,*
>
> *(vii) information about the individual's educational, financial, criminal or employment status or history,*
>
> *(viii) the opinions of a person about the individual, and*
>
> *(ix) the individual's personal views or opinions;*

[16] The ATIPP Coordinating Office of the Department of Justice is the body responsible for the administration of the *Access to Information and Protection of Privacy Act*. It has produced a very useful document entitled "Key Steps When Responding to a Privacy Breach" ("Key Steps," most recently updated in January, 2008) to which I will refer throughout this report. This guide is very similar to documents on the subject produced in Ontario, British Columbia and the federal jurisdiction. Its purpose is to provide a quick guide to public bodies and their employees for use in responding to a privacy breach. It is primarily intended for provincial government departments and agencies, but with appropriate modifications could be equally applicable to other public bodies or, indeed, to private organizations as well.

The "key steps" to which it refers are:

Step 1: Contain the Breach
Step 2: Evaluate the Risks
Step 3: Notification
Step 4: Prevention Strategies

Using this framework I will address each of those steps in turn, and assess the actions taken by WHSCC before, during and after this privacy breach to safeguard the personal information in its custody and control.

Step 1: Containing the Breach

[17] The first step, containment, consists mainly of taking the appropriate common-sense measures to limit or put an end to the breach, such as stopping an unauthorized practice, recovering the records, and correcting weaknesses in physical security. An appropriate individual within the organization should be designated to lead the investigation, and it may be necessary to create a team for this purpose. "Key Steps" also advises that if the breach is unauthorized access to an information technology asset, such as a computer, server or network, that asset must immediately be shut down, and the public body (in the case of a provincial government department or agency) must contact the Office of the Chief Information Officer ("OCIO") which is the provincial government agency responsible for information technology and information management. Step 1 measures also include contacting the police if there is evidence of criminal acts, and deciding who else, externally or internally, needs to be made aware of the situation at this initial stage.

[18] WHSCC became aware of the breach early on January 23, 2008. In consultation with OCIO and other government departments WHSCC immediately created a team, including the Directors of Communications, Information Technology and Health Care Services, and Corporate Counsel, to carry out the investigation.

[19] Early in the investigation it was established that WHSCC's internal computer system had not been accessed. Armed with the preliminary information that had been passed on from the New York security firm, WHSCC began contacting individual suppliers of occupational health and

medical evaluation services. In the course of those contacts WHSCC was advised by a particular company that one of its employees was the individual who had been directly contacted by the security firm. The company further advised that the file-sharing program had been disabled and removed from the laptop the previous evening, and that the laptop was in the company's possession in its St. John's office.

[20] By 3:00 pm on that same day, January 23, 2008 the Commission was also able to speak directly with the New York security firm and confirm the basic facts of the breach, including the very important fact that the file-sharing program was no longer exposing WHSCC files on the internet. As well, by this time the Commission had had a discussion with its own Ottawa-based computer security consultant, Electronic Warfare Associates, and had put together a plan to have EWA conduct an analysis of the laptop hard drive in order to determine, if possible, the extent of the breach.

[21] Actually carrying out that plan was a matter of some complexity. The laptop was not the property of WHSCC but of the private rehabilitation services company. Furthermore, the information on the computer was not solely WHSCC client information, but also information belonging to other government employees and to clients of private companies. It was necessary to reach an agreement among WHSCC, the government and the rehabilitation company on how the matter was to be handled, including an agreement on confidentiality covering all parties who would have access to and would be analyzing the records. However, by 3:00 pm on January 23, 2008 all parties had agreed to the plan, a detailed written confidentiality agreement had been drafted, the laptop had been delivered to the custody of WHSCC, and all of those steps had been properly documented to ensure continuity of evidence. By 10:00 pm on that same day there was a signed contract in place under which EWA was to do the forensic analysis, and the laptop was on its way to EWA by courier.

[22] From the beginning, the WHSCC team had acted in consultation and cooperation with appropriate individuals at the Department of Justice, Eastern Health, OCIO and the rehabilitation services company. By the end of the day on January 23, 2008 detailed briefing notes containing factual background, an assessment of the current status of the matter and an outline of actions required were created for the information of other government officials.

[23] On January 24, 2008 our Office was notified of the breach. It appears that by that point a decision had been made that it was not necessary to contact the police, as it was clear that the breach had been the result of inadvertence, rather than a criminal act or any improper motive.

[24] On January 25, 2008 the first of several news releases came out jointly from WHSCC and the Department of Justice making the details of the privacy breach and investigation public.

[25] It is encouraging to note that by January 23, 2008 WHSCC had already begun preparation of a specific communication to outside service suppliers including rehabilitation centres, chiropractors, physiotherapists and doctors, not only to notify them of the incident, but to remind them of their responsibility to protect the privacy of client information acquired for WHSCC purposes. This kind of action would commonly be thought of as part of Step 4: Prevention (long term safeguards and enhancements) and it is very positive that in this case WHSCC was already considering and implementing prevention steps on the first day of responding to a breach.

[26] In summary, within less than 24 hours the Commission had taken all of the appropriate measures called for under Step 1 for containment of the breach. It had located the source of the breach and determined how it had happened, ensured that it was no longer continuing, recovered the records, and commenced implementation of the necessary measures to prevent similar breaches from taking place.

Step 2: Evaluating the Risks

[27] The second step in responding to a security breach is to evaluate the risks associated with the breach and determine the probable harm resulting from it. There are a number of factors to consider at this point. First, what type of personal information is involved? Generally the more sensitive the information, the higher the risk of harm to individuals. For example, addresses and telephone numbers are often already-published information, and in that case are relatively non-sensitive, whereas health care or credit card numbers, obviously, are much more sensitive because they are potentially usable for identity theft or fraud. Second, it is important to evaluate the extent of the breach: how far has the unauthorized disclosure spread and is there a risk of further exposure? Third, how many individuals are directly affected by the breach and who are they? Finally, what is

the harm that is foreseeable as a result of this breach, not only to the affected individuals, but also to the organization or to the public?

[28] The forensic analysis had identified files containing the personal health information of 108 individuals who were WHSCC clients. In all of those cases, the individual was identified by name, and the file included the individual's WHSCC claim number along with some site measurements and some functional analysis. In roughly one third of the cases the file included the individual's date of birth and claim-related information such as family status, work history, detailed physical assessments, medications, allergies or mental capacity issues. None of this information was encrypted to prevent unauthorized access, nor was it anonymized to break the link between the information and the identifiable individual.

[29] As stated earlier, there were altogether 694 files that had been potentially exposed. It was first necessary to do a preliminary review to determine who "owned" each record. Some files were program files belonging to the contractor. Others contained the personal information of individuals, but the record itself "belonged to" either WHSCC, another government department, the contractor, or an employer client of the contractor. It was necessary to determine ownership in order to determine which body had authority to deal with the information and, in particular, the responsibility for notification.

[30] An individual's personal health information, clearly, is highly sensitive information. While many Canadians accept that their addresses and home phone numbers are shared with the world through the medium of the telephone directory, many of us are reluctant to disclose our age or date of birth, and very few of us would share information such as details of our ailments or medications with any but our closest friends or family. Disclosure of such details could, for most of us, be cause for embarrassment or even humiliation, and would in some cases raise concerns about potential discrimination or other kinds of harm if that information were to become publicly known.

[31] While the disclosure of health information carries with it the risk of personal embarrassment or discrimination there are, however, other kinds of personal information, such as financial or identifying information, and therefore other kinds of risks that the public body must assess. In this case there was apparently no personal financial information, such as credit card or bank account

numbers belonging to any of the affected individuals, in any of the files. Therefore the risk of misuse of the information for fraudulent financial purposes was relatively low.

[32] In some of the files there were, however, items of other personal identifying information, such as MCP numbers. The risk with this kind of information is that it can be used in combination with other information such as name, address, date of birth and other government-issued identification, for the purpose of identity theft. The presence of this sort of information tends to increase the risk. The context of the breach is also important. If the laptop had been stolen, it would be important to evaluate whether the information itself was the target of the theft. In this case, however, the breach was unintentional.

[33] Another factor in the assessment of risk is the likelihood of ongoing exposure. In the present case the cause of the exposure had been determined and stopped, so the exposure was not continuing. However, it was impossible to determine whether any information had actually been downloaded by anyone (other than the security company employee who had reported the breach). Therefore it was impossible to say with absolute certainty how far anyone's personal information may have spread.

[34] In this case, it is also relevant that the personal health information had been collected in the work context of WHSCC-related occupational assessments, but the breach had happened in the social context of an internet music-sharing program. For most of us, the embarrassment or humiliation resulting from exposure of our private health information would be compounded if the recipients were people whom we know or who live in the same community. In this case, however, although the information was exposed on the internet and visible around the world, it is unlikely that there would have been any prior relationship or any other connection between a WHSCC client in Newfoundland and Labrador and a random internet viewer, and so it is less likely that any possible recipient would be in a position to use the information in a way that could cause harm or embarrassment to the subjects.

[35] All of those factors were considered by the WHSCC team. Their conclusion was that in 21 cases there was some risk of identity theft, because of the presence of information such as dates of birth. However, the overall risk of such foreseeable harm as fraud or other financial loss was relatively low.

The main risk to individuals was embarrassment or humiliation if their personal health information was misused.

Step 3: Notification

[36] The third step in responding to a privacy breach is to decide whether anyone should be notified. In a case where there is judged to be very little or no risk of foreseeable harm to individuals or to the public as the result of a breach, then it may well be decided that no notification is necessary. In fact, in some such cases the only result of notifying individuals would be to cause them unnecessary worry and stress. However, where there is any significant potential for harm to an individual whose personal information has been wrongly disclosed, then it is a key principle that the individual ought to be notified, so that he or she will be able to take whatever steps may be necessary to avoid or mitigate the harm. It is also critical that notification takes place within days of the breach, otherwise the opportunity for mitigation is lost. In the present case, the WHSCC team quite reasonably made the decision to notify all of the affected individuals who could be identified with certainty, even though the risk of fraud or identity theft was considered to be low.

[37] In making notification decisions it is not only the risk to individuals that must be considered. There is also the risk of harm to the general public, or to the organization itself, as a result of the breach. In this case there was no apparent risk of harm to public health or safety. There was, however, potentially some risk to the organization. If a privacy breach were to lead to a widespread perception that WHSCC was either negligent or incompetent in its handling of the personal information collected from its clients, then the result would be a loss of confidence or trust in the WHSCC, and this could seriously undermine its ability to carry out its mandate. If an organization tries to conceal or minimize the importance of a privacy breach it can result in an even greater loss of confidence and trust when the attempt to hide the unpleasant facts is revealed.

[38] By contrast, if an organization is perceived to be taking the proper steps to respond to a privacy breach, including promptly and openly notifying affected individuals and the public, it can actually have the effect of increasing public trust and client confidence. At WHSCC it was decided from the beginning to notify the public through media releases about the breach and about what steps were being taken in response. As soon as the WHSCC had sufficient information from the forensic

analysis to complete the risk assessment a notification team was assembled to contact the affected people individually.

[39] The responsibility for notifying affected individuals in the event of a privacy breach ideally falls on the body with the closest direct relationship to the individual. Often this is the body that has collected the information in the first place. In the present case, however, although the body that had collected most of the information was the contractor, it was collected for the purposes of WHSCC programs. The primary relationship was between the affected individuals and the WHSCC, and no doubt most of those individuals regarded the contractor as simply an agent of the WHSCC. In addition, WHSCC had all of the necessary contact information and also had custody of the complete WHSCC file of each individual and so was in the best position to provide the individual with the information he or she needed. Therefore it was WHSCC, not the contractor, who carried out the notification for all WHSCC clients.

[40] For the notification process the WHSCC chose to use the same team of front-line operational staff that had been assembled for the risk assessment. These were experienced staff who had been involved in reviewing all of the files that had been exposed. They were the most familiar with the personal information involved and therefore were best able to answer any specific questions. A phone script and a question and answer document were developed to ensure consistency and accuracy of the information provided.

[41] The 108 individuals who were WHSCC clients were notified by telephone over the next few days. In a few cases they were contacted by letter if they could not be reached by phone. Our Office has been provided with copies of the phone script, the question and answer documents and the protocol developed for the notification process. The thoroughness of the preparation is impressive. For example, the calls were prioritized so that those people whose information was the most sensitive were contacted first. The callers had copies of all of the exposed records that pertained to each individual, so as to be able to state specifically and precisely what information may have been exposed. Each affected individual was provided with copies of the exposed records, and given useful advice to mitigate the possibility of future harm such as financial loss or identity theft. All of the individuals contacted were offered the opportunity to get more extensive advice or counselling.

[42] The majority of individuals who were contacted responded to the notification calmly and with understanding. Some, not unexpectedly, were initially angry. However, only a few took up the offer of more extensive advice or counselling. In the months that have passed since the breach there have been no reports of any of the affected individuals having been victims of fraud, identity theft or any other sort of harm as a result of this privacy breach.

[43] As the "Key Steps" guide states, there are often other parties who should be notified in the event of a privacy breach. If there is any suspicion that a criminal offence has been committed, then the police ought to be notified without delay, and precautions should be taken to avoid destroying or contaminating important evidence. In the present case, as already indicated, it was clear that there was no criminal act or deliberate wrongdoing. The police were therefore not notified.

[44] As outlined above (paragraph 23) the WHSCC from the beginning had acted in consultation and cooperation with appropriate individuals at the Department of Justice, Eastern Health and OCIO. It should be noted that these were the core government bodies whose involvement was necessary, given the circumstances of this particular privacy breach. However, considering that this was the first breach to take place since the privacy provisions of the *ATIPPA* came into force and that it came only a couple of months after a similar, widely-publicized "Limewire" breach at the Public Health Laboratories, it was to be expected that it would receive widespread public and media attention. By the end of the day on January 23, 2008, therefore, detailed briefing notes containing factual background, an assessment of the current status of the matter and an outline of actions required, were created for the information of other government officials who would be expected to respond to public and media inquiries.

[45] On January 25, 2008 the first of several news releases came out jointly from WHSCC and the Department of Justice making the details of the privacy breach and investigation public. As I have stated, WHSCC had decided from the outset that it not only would notify all affected individuals but also would make public the details of the breach and the WHSCC response to it. In my view this was the appropriate decision. It showed that WHSCC was taking responsibility for dealing with the breach and that it was doing so in an open and accountable manner. I have no doubt that public trust and client confidence in the WHSCC have been enhanced as a result.

[46] On January 24, 2008 our Office was notified of the breach by the WHSCC. There is currently no provision in the *ATIPPA* that requires a public body to notify the Office of the Information and Privacy Commissioner in the event of a breach. However, as "Key Steps" advises, organizations are encouraged to do so. First of all, it is quite possible that the Commissioner will be notified in any event as the result of one or more complaints from affected individuals, or simply by reports in the news media. I consider it part of the statutory mandate of this Office, under section 51 of the *ATIPPA*, to independently investigate privacy breaches if such an investigation appears to be warranted, in order to report to the public on matters of importance and to make recommendations to ensure compliance with the *Act*. Early reporting to us by the public body responsible for the breach will better enable us to respond to inquiries.

[47] In addition, it is possible that if our Office is notified in the early stages of responding to a breach, we may be in a position to offer advice and guidance to a public body if it is experiencing some uncertainty about how to proceed. This is particularly true in the case of smaller bodies that may not have many resources to commit to responding to a privacy breach.

[48] As I have stated previously, public trust and confidence are always potentially in jeopardy when a privacy breach takes place. Prompt notification of the Commissioner will invariably be perceived as more open and more responsible, whereas a failure to notify, especially where the breach is a serious one, risks leaving the public with the contrary impression.

[49] It is also important because our Office may be in a position to identify problems of a more systemic nature that may exist within an organization and may need to be addressed. For all of these reasons it is my view that it is a good practice to notify this Office whenever there is a privacy breach of any significance.

[50] I wish to add that, just as not every privacy breach requires notification to affected individuals, not every privacy breach needs to be reported to the Commissioner. First, it is of course only a privacy breach under the *ATIPPA* that will activate our statutory mandate. Second, there are factors relating to the seriousness of the breach that may affect the decision whether or not to notify us. In the present case, it is my conclusion that the WHSCC made the appropriate decision to report the breach to our Office right away, and is to be commended for that decision. In the circumstances of

this case it demonstrates a high level of commitment to accountability and to developing a high standard of privacy protection within the organization.

[51] One final aspect of the notification process deserves mention. It appears from the telephone notification script and other documentation that the affected individuals were not advised by the WHSCC during the notification process that they could contact the Office of the Information and Privacy Commissioner to file a complaint. The "Key Steps" guide recommends that this advice along with the necessary contact information be provided as part of the notification process. It helps to restore the confidence of affected individuals if they are informed that there is an independent agency to which they can go to make a complaint and ask for an investigation, even if they do not actually go on to take such action. WHSCC accepts the value of including this information in the notification process and acknowledges that the failure to do so was an oversight.

Step 4: Prevention Strategies

[52] All of the above – Step 1 (containment), Step 2 (risk evaluation) and Step 3 (notification) – were completed within two weeks from the day that the WHSCC found out about the breach. The fourth step, prevention, requires the body to take the time to systematically review the causes of the breach and decide whether there are lessons to be learned from it. This final stage may involve any or all of the following components:

- a physical, technical and administrative security audit;
- a review of policies and procedures, especially those that are relevant to the breach, and the development or improvement of safeguards to prevent further breaches;
- a review of employee training practices;
- a review of the practices of service delivery partners.

Potentially, the lessons learned may result in a prevention plan, and there may be an audit at the end of the process to ensure that the plan has been put into effect. Step 4 is therefore critical for ensuring that similar breaches do not occur in future.

[53] As WHSCC itself has pointed out in discussions and correspondence with this Office, there were at least three different sets of rules that applied to the circumstances of this particular privacy breach, each of which potentially could have been expected to prevent it from occurring: the *ATIPPA,* Part IV, which governs protection of privacy, and which applied to WHSCC; the federal *Personal Information Protection and Electronic Documents Act ("PIPEDA")* which applied to the private contractor; and the contractor's policies together with the occupational therapist's professional code of conduct, which applied to the employee.

Jurisdiction

[54] In paragraph 12, above, I referred to a comment made by WHSCC in its letter requesting this review, regarding the potentially limited jurisdiction of this Office to investigate the breach. The contractor, as a private organization is not included in the definition of a "public body" under the *ATIPPA,* and is not subject to that provincial *Act.* Rather, it is subject to *PIPEDA*, and therefore to the oversight jurisdiction of the federal Privacy Commissioner of Canada. That federal legislation is different from the *ATIPPA* but is directed toward similar problems and has a similar purpose: to establish rules to govern the collection, use and disclosure of personal information. For similar privacy breach situations, the protective and preventive measures expected under both regimes would be much the same. In fact, the Privacy Commissioner of Canada has published a guide for responding to a privacy breach that is very similar to "Key Steps." In both guides the recommended steps to take in responding to a breach are the same. The governing principles are the same, and the results of an investigation would be similar, because under either statute, organizations dealing with the personal information of individuals are held to the same standards.

[55] Our Office has no jurisdiction to directly review a contractor's compliance with *PIPEDA*. That jurisdiction lies with the Privacy Commissioner of Canada. However, the contractor's work was carried out for and at the request of WHSCC. (It also did work for some other clients as well, but that is beyond the scope of this report). It was the Commission that entered into a contract for the occupational therapy assessments to be done and consequently for the records to be created. The information was to be collected from the individual clients of the Commission under the authority of the *Workplace Health, Safety and Compensation Act,* and provided to the Commission under the terms of the contract. Therefore although the records were not, at the time of the breach, in the physical

custody of the WHSCC, it is clear from the provisions of the contract that they were under its control. Ultimate responsibility for safeguarding the security of the personal information of WHSCC clients was with the Commission.

[56] The *ATIPPA* provides, in section 5, that it applies to all records in the custody of *or* under the control of a public body. Section 7, setting out the right of access to records, and section 52, giving this Office the right to require records relevant to an investigation, similarly refer to records in the custody of *or* under the control of a public body. Therefore our responsibility under the *ATIPPA* in this and similar cases extends beyond the location, organizational structure and records held by the public body itself, to the information that is ultimately under the public body's control, regardless of where physical custody of the records may reside.

[57] The jurisdictional divide, therefore, is not really a difficulty in the circumstances of this case. It is within our mandate to review the policies and practices of the WHSCC itself relating to the collection, use, disclosure and safeguarding of personal information, and it is also our mandate to review the terms and conditions of WHSCC contracts with outside service providers relating to those same matters. We may draw conclusions and make recommendations with respect to the adequacy of those contracts for the protection of the privacy of WHSCC clients and the safeguarding of their personal information.

Reasonable Security Arrangements

[58] The privacy provisions of the *ATIPPA* (Part IV) had been proclaimed on January 16, 2008, just five days prior to the breach, but the *Act* had been passed in January 2005, and all of its other provisions had been in force since then. Public bodies in Newfoundland and Labrador had effectively been given three years to prepare themselves for the coming into force of Part IV. Under Part IV, a public body may only collect, use and disclose personal information for limited purposes, and has a statutory obligation to protect personal information from unauthorized use or disclosure.

[59] The core protection principle in Part IV is section 36, which reads as follows:

> *36. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

[60] I have discussed section 36 in a number of previous reports, beginning with Report P-2008-001, the very first privacy report issued by this Office. Section 36 requires public bodies to make "reasonable security arrangements." As I have previously commented, the standard imposed on public bodies is not perfection. That would be impossible. However, the standard is also not a subjective one. What constitutes objectively reasonable security measures will depend on the circumstances, and will involve an assessment of such factors as the foreseeability of the breach, the seriousness of any anticipated harm, the cost of alternative security arrangements and relevant standards of practice.

Foreseeability

[61] The actual breach was not only foreseeable; it was actually foreseen. There had been a previous similar incident, in November 2007, in which an employee of the Public Health Laboratory ("PHL") had installed a file-sharing program and had exposed personal health information on the internet as a result. This incident received widespread publicity, and our Office subsequently carried out an investigation (see Report P-2008-001, which was released in June 2008).

[62] Following the November 2007 PHL incident, OCIO had immediately begun a number of initiatives to strengthen data security in similar situations within its own jurisdiction. Some of those measures are directly relevant to the present matter. File-sharing and instant messaging programs were no longer permitted on government-owned computers because of their vulnerability to deliberate or accidental exposures. All OCIO contractors were required to have confidentiality agreements in place in order to continue to work for OCIO on government systems. A campaign to raise awareness of the need for vigilance about information security was carried out during the months following the PHL breach.

[63] Following the January 2008 WHSCC breach, government directed all departments and agencies that had not already done so to implement the OCIO measures. The government also required that all government contractors be required to have confidentiality agreements in place, like OCIO had done, in order to continue to work for government. WHSCC had in fact already taken those steps. WHSCC was aware of and had participated in the earlier initiatives, and had a policy in place before the 2008 breach, barring all employees from installing file-sharing programs on WHSCC computers.

Unfortunately that specific requirement did not at that time form a provision of the contracts with outside service providers and so the measures taken by WHSCC were not sufficient to prevent this particular breach.

WHSCC's Existing Policies and Practices

[64] At the time of the breach the WHSCC had a set of fairly comprehensive policies and procedures dealing with information access and protection and electronic information security. Those had all been drafted and put in place prior to the proclamation of the *ATIPPA*, though several of them date from 2004 and reference the soon-to-be-proclaimed *Act*. I will briefly describe the more important ones for the purposes of this report.

[65] The Commission's General Policy GP-01 (effective 1998) was in place at the time of the breach, and deals with Information Protection and Access. It is a comprehensive statement of the application of access and privacy principles, and references confidentiality, the sensitive nature of client information, the need to balance privacy against the need to share information. It covers access to claim file information by the worker and others, including employers and health care providers, access to employer assessment files, and sharing information under statutory authority or court orders. Although it is somewhat dated, referencing the *Freedom of Information Act* (the predecessor of the *ATIPPA*) the principles are sound and it provided a reasonable foundation for other information access and privacy protection policies and procedures.

[66] Procedure HR 11-08 dates from March 2004, and is a human resources procedure on information security which references Policy GP-01, and also the *ATIPPA*. It defines the responsibilities of Commission employees, and applies to all information created, received and distributed by employees of the Commission. It includes sections on:

- the use and control of information, defining how decisions are made about access, how information is used, and how retention and disposal decisions are made;
- determining internal access to information;

- general practices related to non-public information, including such things as removal of information from Commission premises, use of laptops and other portable devices, discussion of non-public information in public places;
- the use of information technology and equipment, including passwords, unauthorized access, downloading or use of unauthorized software, and e-mail; and
- reporting information security incidents and viruses.

[67] Procedure ITS-300, which also dates from March 2004 and references the *ATIPPA*, is an Information Technology Services procedure on the management of e-mail. It is a comprehensive guide to the place of e-mail records within the Commission's records management procedures, and includes important sections on user responsibilities and on privacy and security.

[68] I have concluded that WHSCC's own policies and practices, particularly the ones referred to above, could have effectively prevented a privacy breach like this from occurring within WHSCC itself. Employees of the Commission were not permitted to download unauthorized programs onto WHSCC computers. File-sharing or instant messaging programs were specifically not permitted. There was also a policy of strictly limiting the information that could be saved on Commission laptops, and how laptops were to be handled and stored. This policy recognized that information on WHSCC systems was not currently encrypted, and therefore required that laptops have power-on and hard drive passwords installed so that, in the event of loss or theft, unauthorized persons could not easily gain access to the information on them.

[69] WHSCC's existing policies therefore covered most of the foreseeable possibilities. However, they did so only for the Commission's own databases, its own employees and its own sites. Although they were relatively comprehensive and up to date, they did not translate into the contracts that WHSCC had with outside service providers or to the policies and actual practices followed by contractors in the course of their day-to-day work.

Contracts with Outside Service Providers

[70] All health care and rehabilitation services for WHSCC clients are actually provided by outside service providers such as physiotherapy clinics. At the time of the breach WHSCC had a Memorandum of Agreement with each of the major health care provider groups in Newfoundland and Labrador, and contracts with each individual service provider. The contract between the WHSCC and the particular occupational rehabilitation service provider involved in this case had been signed on March 29, 2007. This form of contract had been in use for some time, and would be considered a relatively standard and comprehensive contract for the provision of services. It is over 20 pages in length, with another 20 pages of appendices. It prescribes the services to be provided to the Commission by the contractor, the terms of payment, terms regarding the qualifications of the contractor's employees, safety, insurance, dispute resolution and so on. The appendices cover, in greater detail, rules regarding provision of service, service standards, payments, and confidentiality.

[71] One clause in the main contract provides that the contractor is required to observe the requirements for confidentiality and conflict of interest as set out in a schedule to the contract. That schedule is only one page long, half of which is devoted to conflict of interest rules. The confidentiality portion simply provides that the contractor recognizes the Commission's policy on release of information, while maintaining professional standards in terms of confidential information, and also provides that the contractor is not to use any information gathered in the course of providing services under the agreement without consent of the Commission and affected parties.

[72] In short, the contract with the Commission required the contractor to keep the personal information of WHSCC clients confidential, but did not offer any guidance on how this would be done. In addition, it did not contain any provision for what the contractor should do in the event of a privacy breach.

Responsibility of Employees

[73] It is appropriate at this point to say a few words about the responsibility of individual employees in incidents like this. The employee involved in this breach was an occupational therapist, whose professional activities are licensed by the provincial Occupational Therapy Board. The Board

establishes educational and professional qualifications and standards, licences therapists, handles complaints, and imposes discipline for misconduct. It has issued standards of practice, and the occupational therapist was required to comply with them. Those standards in various places refer to the need to protect client privacy and dignity, to confidentiality, and to appropriate access to records. However, those standards are statements of general principle, and do not necessarily provide concrete guidance to an individual in practical day-to-day professional activities.

[74] In such circumstances it is not enough for us to simply declare that employees are responsible for safeguarding the information they handle. Proper orientation and ongoing training are critical, and it is the responsibility of an employer to ensure that they are provided to its employees. Each public body is responsible for ensuring that its own employees are adequately educated and trained with respect to matters such as privacy, confidentiality, information handling practices and the security and integrity of records. But how does a public body ensure that training is adequate and up to date for the employees of another organization with which it has a contractual relationship? In a situation where the public body does not have day-to-day supervision of those employees and control and direction of their activities, it is difficult. The WHSCC contract provided that the contractor had to ensure that all employees had appropriate educational qualifications, and had to satisfy WHSCC of those. The contracts did not, however provide specifically for privacy training for the contractor's employees.

[75] The result was that while the WHSCC had policies that covered confidentiality, privacy and information security in some considerable detail, and had, for example, specifically barred the installation of file-sharing programs on WHSCC computers, there was no assurance that the content of those policies and rules would be shared with the contractor or the contractor's employees. In those circumstances, it is hard to attribute fault to an employee who, without proper privacy training, could not have been expected to anticipate the harm that could result from installing a file-sharing program on a workplace computer.

Cost of Prevention Measures

[76] Cost is sometimes a relevant factor in assessing breach prevention measures, especially where physical or technical security is the problem. This is not really a major factor here. The preventive

measures required to deal with this sort of breach would mainly be the development and improvement of policies, implementation of concrete rules and procedures in response to previously unforeseen risks, and above all employee training. Training is a cost item, of course, and may be a big one for smaller organizations, but an organization like WHSCC or a government department conducts training for its staff on a variety of work-related topics, and it is a normal part of the "cost of doing business." Put in the context of the overall training budget for an organization, privacy training should not add much. An organization like WHSCC is big enough to conduct its own targeted privacy training in-house, and as we will see, it does so. In addition, training on information security and privacy is available elsewhere within government, for example from OCIO, or from the ATIPP Coordinating Office. For small contractors, the situation is somewhat different, but perhaps their employees ought to be able to take advantage of WHSCC or other government training programs.

III NEW MEASURES TAKEN BY WHSCC FOLLOWING THE BREACH

Standard of Practice – the Multi-layered Approach

[77] In Report P-2008-002 I discussed at length the conclusions of Information and Privacy Commissioners and information technology professionals across the country about the need for multiple layers of security when attempting to protect personal information. I will not repeat that discussion here. It is sufficient to note that a multi-layered approach, consisting of physical, administrative and technological measures, is now the minimum standard of accountability for public bodies that have custody or control of personal information.

[78] It is worth noting as well that best practices are continually changing. It is not sufficient for an organization to put in place a set of reasonably acceptable measures. It will also need a policy in place that provides for review and timely updating of those measures.

Physical Measures

[79] Physical measures to protect the personal information in its custody, such as locked filing cabinets, restricted access to offices through use of electronic photo ID cards, and security guards

were already in place at WHSCC, and similarly at the contractor's offices. Those factors did not play a role in this breach.

Administrative Measures

[80] Immediately following the breach, WHSCC sent a memo to all employees listing a large number of practices that must be followed. It included such things as copying personal information to portable storage devices such as CD's or USB drives only if they were encrypted, not working on WHSCC data files on computers not owned by the Commission, not using file-sharing programs and so on. Many of these measures were already in place, but the memo served as a reminder, and it also advised all staff that they were responsible for making themselves aware of relevant legislation and policies. A similar memo was sent to all contractors.

[81] WHSCC subsequently sent more detailed letters to all contract service providers reminding them of their responsibilities for protecting the information of Commission clients. The letter requested that the contractor review all security measures, including policies and practices with regard to computers and access. In particular, it warned about file-sharing programs and stated that such programs should be strictly prohibited on computers that store confidential information. It also asked that each contractor have all of its employees sign a new and updated Declaration of Confidentiality.

[82] Immediately following the breach, the Department of Justice was asked to review the language of the existing contracts with service providers and recommend changes. In the meantime, the Commission's legal staff developed interim provisions, to be used in the event that contracts came up for renewal.

[83] The Department of Justice drafted new contract language, which it provided to WHSCC in May 2008, covering confidentiality, materials and copyright. From the *ATIPPA* privacy perspective the

new language is a great improvement on that of the old contract. Confidential information is defined quite broadly, and includes personal information as it is defined in the *ATIPPA*. The provisions respecting the contractor's obligations relating to confidential information reflect the structure and

content of Part IV of the *ATIPPA,* which limits the collection, use and disclosure of personal information. In addition, the new contract language contains provisions describing the level of physical and electronic security that the contractor must provide, and requiring the contractor to establish and maintain adequate security policies, standards and safeguards.

[84] The contractor is also required to notify the Commission of any privacy breach or unauthorized possession of confidential information, to assist in the investigation and to follow the "Key Steps" protocol in the event of a breach. This new contract language has systematically replaced the old as contracts come up for renewal, and it appears that this process will be complete by the end of 2010.

[85] The new contract language requires the contractor to ensure that its employees comply with all policies, standards and safeguards that it establishes. It does not, however, deal with the issue of privacy training for contractor employees. This is a concern, because in my view it represents a potentially significant gap that still exists between the adoption of adequate and up-to-date privacy policies and practices, and their effective implementation.

[86] Prior to the breach, WHSCC's basic training for new staff had always involved a component on confidentiality. Basic privacy training was incorporated in 2004 in anticipation of the *ATIPPA*, when management training was also included. At the time of the breach, Commission staff were in the process of receiving a series of privacy training sessions provided by the ATIPP Coordinating Office.

[87] Following the breach, WHSCC developed its own new privacy training program which brought together all of the components of privacy in Commission policies. This training session was provided to all Commission staff in 2008. Based on an exposition of the Canadian Standards Association *Model Code for the Protection of Personal Information*, it incorporated a review of the *ATIPPA*, the WHSCC's General Policy GP-01 and the Information Security Procedure, described earlier in this report.

[88] In addition, the WHSCC Human Resources department has developed a training session focused specifically on the protection of personal information. Three-quarters of WHSCC staff attended that training session in 2008; the remainder received it in 2009. During the same period the

majority of staff completed the on-line privacy training sessions provided by the ATIPP Coordinating Office. The Commission's legal department has also developed a privacy breach training session, which is being presented to staff at unit meetings. The Commission has also made provision for this training to be provided to new employees.

Other Initiatives

[89] In 2008 the Commission formed a Privacy Steering Committee to provide leadership and direction regarding privacy issues. The committee developed a Privacy Action Plan to identify and track privacy initiatives and accomplishments. Among other things the 2008 Action Plan provided for privacy training for all Commission staff, as indicated above, and initiated the practice of making privacy a standing agenda item for all departmental and unit meetings, in order to promote privacy awareness and share best practices. The Privacy Steering Committee has become a permanent committee and the Action Plan has become a permanent process, reviewed and updated quarterly at both the corporate-wide and departmental levels.

[90] Prior to the breach, the Commission's approach to developing a culture of privacy was often a top-down process, in which a small number of people developed plans or policies to communicate to the rest of the organization. With the creation of the Privacy Action Plan, the Commission has adopted an approach that strives to involve everyone. This has resulted in better solutions to problems, better discussion at meetings, and better training. In particular, the Commission has acknowledged that it is natural that individuals sometimes make mistakes, and has concluded that rather than taking disciplinary action in response to errors, a "lessons learned and prevention" approach produces better results.

[91] In the period since the adoption of the Action Plan the WHSCC has conducted a corporate-wide risk assessment review. The discussions at the unit-level meetings that followed have eliminated a number of administrative practices that were identified. Those included such very concrete steps as the elimination of paper clips or the addition of a "double-check" step in sending out files to cut down on misdirected documents, or using only pre-programmed fax numbers that have already been tested for accuracy to transmit confidential information. Another example is the establishment of a corporate-wide protocol for client identification at the beginning of every

telephone, e-mail or in-person conversation to ensure that personal information is not mistakenly discussed with the wrong person. Many similar remedial or enhancement measures are only discovered as a result of grassroots staff involvement.

[92] It has been recognized that organizations that handle personal and confidential information must have frequent reviews of their information management and privacy policies in light of technical developments. WHSCC has adopted policies and practices to ensure the timely updating of breach prevention measures.

[93] The Commission's Policy GP-01, referred to above in the section on existing policies, was completely revised in June 2009 at the behest of the Privacy Steering Committee. It is now titled Information Protection, Access and Disclosure, and its preamble incorporates the Ten Privacy Principles developed by the Canadian Standards Association. Whereas the old policy referenced the *Freedom of Information Act*, the new one closely follows the requirements and principles of the *ATIPPA*. It represents a timely and substantial improvement to the basic policy document governing information protection, access and disclosure. Following Board approval further training was developed for all staff in order to introduce and explain the new policy.

[94] The WHSCC, like other public bodies in the province, is in the process of reviewing the obligations and responsibilities it will have under the *Personal Health Information Act* (SNL 2008 c. P-7.01 – the *"PHIA"*) which is expected to be proclaimed in the near future. Many of the contractual service providers, as well as the WHSCC itself, will be considered custodians of health information under the *PHIA*.

Technical Measures

[95] Technical barriers to installation of potentially harmful software have been installed on WHSCC equipment. Now, not only does policy prohibit the installation of file-sharing programs, there are controls that prevent such programs from operating. Immediately following the breach, the contractor involved with the breach implemented the same measures. Subsequently, those measures were incorporated into the new contract language for all contractors.

[96] Encryption is now the minimum acceptable standard for all mobile devices such as laptop computers and portable USB drives that contain personal information files. Following the breach, WHSCC revised its e-mail policy to require the use of encryption when personal or confidential information had to be sent via e-mail. WHSCC subsequently adopted an encryption policy for the use of portable storage devices by its own employees.

[97] The contractor involved in the breach installed encryption software on its own computers in order to encrypt all data files, shortly after the breach. A requirement for the encryption of all confidential information on portable storage devices was made a part of the new contract language for service providers.

[98] At the beginning of my discussion of Step 4 (prevention strategies) I commented that the lessons learned by an organization in the course of reviewing the causes of a privacy breach may result in a prevention plan, and there may be an audit at the end of the process to ensure that the plan has been put into effect. Clearly, this has been the case with the WHSCC. There is now a permanent Privacy Steering Committee, and it appears to me, from the documents provided, that the ongoing Privacy Action Plan is comprehensive in scope and very concrete. Because of the way in which it is organized, the Plan itself constitutes a systematic, periodic review of information security, of privacy policies and procedures, of training practices and of the relationship with service delivery partners. Furthermore, it operates on both the corporate-wide and unit levels, and it is an appropriate vehicle by which new developments such as the responsibilities associated with the proclamation of the *PHIA* can be incorporated into the policy framework.

[99] In some ways an ongoing Privacy Action Plan with a permanent review framework such as the WHSCC has implemented is superior to a one-time end-of-review audit, as it embodies the idea of a culture of privacy in organizational form. Clearly, with privacy as an agenda item at all corporate-wide and departmental meetings, the Commission's managers will be in a position to continuously evaluate whether Commission policies are up to date, whether Commission employees are adequately trained, and whether Commission practices reflect policy. Such a process requires that it be adopted and supported at the highest organizational levels to be successful, and clearly that appears to be the case at the WHSCC.

[100] The situation with respect to outside contractual service providers is a different matter. It is clear that WHSCC has made great strides in incorporating privacy requirements into the language of the contracts, and since the breach has done an exemplary job of communicating the seriousness of privacy breaches and the necessity of taking concrete steps to avoid it happening again. However, the extent to which contractors have understood the message, armed themselves with the necessary knowledge, and upgraded their own policies and practices to comply with the new contractual requirements is less clear. At present there is no formal audit mechanism to evaluate contractor compliance. However, WHSCC acknowledges that it is the responsibility of the Commission, and specifically its managers and directors, to ensure satisfactory compliance by contractors with the Commission's policies.

[101] The proclamation of the *Personal Health Information Act* will significantly affect this issue. The WHSCC and its contractual service providers will all be considered custodians of personal health information under the *PHIA* and will have similar statutory responsibilities under that *Act*, although there will still reside with WHSCC a greater degree of accountability for protection of the information which is under WHSCC's control.

V CONCLUSIONS

[102] Following the "Key Steps" framework, my conclusions after assessing the actions taken by the WHSCC before, during and after the privacy breach to safeguard the personal information of its clients in its custody and control may be stated succinctly. Within less than 24 hours the Commission had taken all of the steps called for under Step 1 for containment of the breach. Within less than two weeks the Commission had appropriately evaluated the risk of harm to the affected persons and had notified them all individually. The WHSCC wisely chose to make the details of the breach and the investigation public in order to enhance public trust and client confidence. It also is to be commended for notifying our Office at an early stage.

[103] The Commission's existing policies and procedures were dated but sound, and would have effectively prevented the breach within the WHSCC itself. Following the earlier PHL incident, the WHSCC had in fact taken steps to prohibit the installation of file-sharing programs. The weaknesses

that existed were primarily in the area of the contracts with outside service providers, which prior to the breach did not offer concrete guidance on privacy and confidentiality.

[104] The prevention measures taken by WHSCC following the breach were swift and comprehensive, and in my view were appropriate. Immediate administrative and technical measures ensured that similar breaches could not happen again. New contract language systematically upgraded the requirements for contractors, and the contract renewal process is almost complete. The Commission has taken further technical measures such as requiring the encryption of personal information on portable storage devices. There are new privacy training programs to make sure that staff are armed with the necessary knowledge and attitudes.

[105] Perhaps most importantly, the establishment of a permanent Privacy Steering Committee and an ongoing Privacy Action Plan has resulted not only in a completely revised Information Protection, Access and Disclosure Policy, but also in a corporate-wide risk assessment review, and the continuing implementation of enhanced privacy and security measures as a result of grassroots staff involvement. The Commission has stated, with justification, that as a result of these changes there has been a culture shift from an environment in which privacy protection was already highly valued, to one in which the CSA 10 Principles of Privacy are being incorporated into all areas of information management.

[106] My remaining concerns are not with the privacy, confidentiality and security environment within the Commission, but with the policies and practices of the outside service providers. They themselves, as I have already stated, are under federal jurisdiction. However, the personal information of WHSCC clients that is provisionally in the custody of the contractors is, in the last analysis, under the control of the Commission, and the Commission therefore has an ongoing responsibility to take whatever reasonable measures are available to it to safeguard that information in order to protect the privacy of its clients. The Commission has already taken such steps, particularly in the matter of substantially improved contract language. It remains to be seen whether those contractual obligations will be sufficient to motivate contractors to establish appropriate policies and practices, and to provide adequate training to their own employees.

[107] Overall I conclude that prior to the breach the WHSCC had made reasonable security arrangements within the meaning of section 36 of the *ATIPPA* to protect the personal information of its clients against foreseeable risks. Following the breach, the WHSCC has taken reasonable measures to review the causes of the breach and to strengthen its policies, procedures and practices so as to minimize the risk of future such incidents.

VI RECOMMENDATIONS

[108] In view of my conclusions and concerns, I have only two recommendations to offer.

[109] First, the Commission should consider, in light of its own responsibilities to safeguard the personal information of its clients, whether it would be reasonable to conduct an audit of its contractual service providers, or some sample of them, in order to gauge the extent of their compliance with the policies and rules of the Commission, the terms of their contracts and accepted standards of privacy practice, and to take any action that appears to be necessary as a result. Such an audit could possibly become a term of service provider contracts.

[110] Second, the Commission should consider, either independently or together with any action it may undertake in response to my first recommendation, whether it would be reasonable to set a concrete contractual standard for privacy training for the employees of contractors, and to assist in the provision of that training.

[111] I wish to add that neither of the above recommendations should be considered as a criticism of the Commission. Rather, they are intended to be constructive assistance, as measures that could potentially further enhance the Commission's ability to carry out its responsibilities under the *ATIPPA*. The Commission is in the best position to evaluate these recommendations and to take further action as it sees fit.

Dated at St. John's, in the Province of Newfoundland and Labrador, this 29th day of March, 2010.

E. P. Ring
Information and Privacy Commissioner
Newfoundland and Labrador