June 25, 2008 **P-2008-001**

NEWFOUNDLAND AND LABRADOR

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

REPORT P-2008-001

Department of Health and Community Services

Summary: On 20 November 2007 a privacy breach occurred involving the accidental disclosure over the internet of personal information of patients and staff from a computer operated by a Consultant working for the Public Health Laboratory ("PHL"), which is the responsibility of the Department of Health and Community Services ("DHCS"). DHCS followed up by assessing the severity of the breach and contacting a number of affected individuals. DHCS also notified this Office of the breach, and on 28 November 2007 requested that we accept for investigation any complaints from affected individuals who received DHCS's notification, despite the fact that the privacy provisions of the *ATIPPA* were not yet in force. This Office agreed to do so. Three complaints were subsequently received.

The Commissioner commended DHCS for its response to the breach, including its notification process. The Commissioner further commended DHCS for requesting that this Office investigate any complaints, despite the privacy provisions of the *ATIPPA* not being in force at the time of the breach. The Commissioner found, however, that policies governing the management, retention and destruction of electronic records were significantly lacking at PHL, and that areas of responsibility for electronic records and privacy between PHL and Eastern Health (which provides information technology support to PHL) have not been formalized appropriately. The Commissioner also determined that appropriate training had not been provided to staff or management of PHL prior to the privacy breach, and that such training should be provided at the earliest opportunity. The Commissioner further recommended that privacy protection be built into the contractual language whenever a third party is retained to provide services to PHL; that Privacy Impact Assessments be conducted where appropriate at PHL; and that recommendations of the IT Security Framework Review be implemented.

Statutes Cited: *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A 1.1, as am. s. 36.

Authorities Cited: British Columbia OIPC Investigation Report F06-01

Other Resources:
- *Introduction to Key Steps for Organizations in Responding to Privacy Breaches*, Office of the Privacy Commissioner of Canada http://www.privcom.gc.ca/information/guide/index_e.asp
- *Key Steps When Responding to a Privacy Breach*, & *ATIPP Privacy Policy and Procedures Manual*, ATIPP Office, Department of Justice, Government of Newfoundland and Labrador http://www.justice.gov.nl.ca/just/civil/atipp/
- *Privacy Audit – A Compliance Review Tool*, Office of the Information and Privacy Commissioner, Newfoundland and Labrador http://www.oipc.gov.nl.ca/pdf/NLOIPCPIA.pdf

I BACKGROUND

[1] On 22 November 2007 officials of the Department of Health & Community Services ("DHCS") advised this Office that a privacy breach involving patient records had occurred at the Newfoundland and Labrador Public Health Laboratory ("PHL") on 20 November 2007. A further briefing was provided to this Office by DHCS on 28 November 2007. It was acknowledged by DHCS and this Office that the privacy provisions of the *Access to Information and Protection of Privacy Act (the "ATIPPA")* were not yet in force, however DHCS requested permission to include in its letter of notification to affected individuals that those individuals may ask our Office to investigate any complaints they may have. The Commissioner (my predecessor) agreed that this Office would accept any complaints for investigation, and three such complaints were subsequently received.

[2] The information involved in the breach included names of individual patients, as well as gender, age, MCP number, physician name, hospital or clinic location. This information was listed along with data pertaining to test results for several illnesses and conditions such as C. Difficile, RSV, Rubella, Hepatitis A & B, Parvovirus, and HIV.

[3] All three complainants expressed that their right to privacy was compromised through this breach. One individual, after receiving notification of the breach, stated as follows:

> *I am extremely fearful for myself and those I love due to the stigma surrounding this illness. I have experienced undue hardship at the hand of a previous landlord and members of the community, when they discovered I was ill with HIV.*

[4] The mandate of the Public Health Laboratory is to act as the provincial laboratory centre for infectious disease surveillance and control; to provide a comprehensive range of specialized and reference laboratory services in clinical and public health microbiology and infectious disease epidemiology to the province; and to pursue research and development in these areas. The PHL is the responsibility of the Department of Health and Community Services. Information technology services for PHL are provided by Eastern Health. The Public Health Laboratory is a

separate and distinct entity from other laboratories operated by Eastern Health which are located in different health care facilities.

[5] In terms of corporate governance, this Office has been advised by DHCS that PHL is a division of DHCS, but it has a "unique relationship" with Eastern Health. The Director of the PHL is employed by and reports to DHCS, while all other staff are Eastern Health employees. In addition, Eastern Health provides human resource, purchasing, housekeeping, infrastructure, IT and financial management services for PHL. DHCS says that PHL's organizational structure is under review.

[6] Eastern Health is the largest integrated health organization in Newfoundland and Labrador serving a regional population of more than 290,000 and offering tertiary or high-level health care services province-wide. It was created in 2005 as a result of the merger of seven health care organizations.

[7] The details of this privacy breach were widely reported in the media at the time. Essentially, a long-time employee of PHL (the "Consultant") retired in June 2007, but PHL retained her on a contract to work from home for the purpose of concluding a long-standing project which she had been working on. It was determined that she would need the use of a computer at home in order to do this work, so she was allowed to take with her the computer which she herself had used at PHL.

[8] On the evening of 20 November 2007 the Consultant, while using the computer at home, installed a file-sharing program called Limewire Pro, which is a type of file sharing software used for downloading music from the internet. She then began the process of downloading music selections, but discontinued before any selections were actually downloaded. She decided not to proceed after a text box appeared which referenced license requirements. Shortly thereafter, she received a telephone call from a representative of an investigation company in New York who had encountered a number of files containing personal information, which he believed had been exposed on the internet through the Consultant's computer. The Consultant followed instructions from the New York company in order to immediately cease transmittal of the information over

the internet. The Consultant then proceeded to immediately notify senior management of PHL. A contact was made by PHL management to a senior person with the Office of the Chief Information Officer (the "OCIO") requesting advice and assistance, and from that point onwards OCIO was engaged, together with the Department of Health and Community Services, PHL and Eastern Health, in responding to the privacy breach. The OCIO operates as an entity within Executive Council, and provides information management and information technology support for many government departments, boards, commissions and agencies.

[9] The New York company reported that "approximately" 1,400 files originating from the Consultant's computer were disclosed through Limewire. Limewire allows individuals to share songs stored on their computer with all other Limewire users. An individual Limewire user can then choose song selections from the entire catalogue of songs of all Limewire users. The New York company indicated that instead of sharing files from her "shared music" folder, the Consultant must have inadvertently set up Limewire in such a way that her shared files were from the "my documents" folder instead, which made all of the files in her "my documents" folder available over the internet.

[10] DHCS contracted with an Ontario-based consulting company called Electronic Warfare Associates ("EWA") to conduct a forensic audit of the Consultant's computer in order to determine the extent of inappropriate access. EWA concluded that a total of 1,420 files had been "made available" through Limewire, including personal files of the Consultant as well as PHL records such as meeting minutes, a red tape reduction report, a briefing note, etc. Most importantly, however, the files also contained the personal information of staff and patients. EWA also concluded that most of the 1,400 files were not likely shared. They were able to determine that a total of 375 files were accessed by another party after Limewire was set up. They also indicated that it is not possible to determine who may have accessed those files, although EWA reported that the New York company indicated that it had downloaded 178 of those files. EWA noted that there was a small possibility that all 1,420 files may have been available for downloading during a brief 111 second period of time during the set up phase of Limewire when the files designated for sharing were being indexed by the program. EWA indicated that the probability of access for these files would be quite low given the brief interval.

Of the 375 files which are known to have been accessed, a team representing PHL, OCIO and DHCS (the "team") reviewed the files to determine the type of information which was disclosed and to determine what follow-up action would be required.

IV DISCUSSION

[11] As noted above, no violation of the privacy provisions of the *ATIPPA* can be deemed to have occurred as a result of this investigation because the privacy breach occurred approximately eight weeks prior to those provisions coming into force on 16 January 2008. Be that as it may, I think it would be useful for all parties to frame my discussion with some reference to the *ATIPPA* privacy provisions, so that the public bodies, the affected individuals, as well as the general public and media will be able to see from this report how those provisions will likely be applied to future privacy breaches.

[12] The key section of the *ATIPPA* in relation to this privacy breach is section 36, which is 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.*

[13] It is important to note the use of the term "reasonable" in section 36. The Information and Privacy Commissioner for British Columbia, in Investigation Report F06-01, commented on the concept of reasonableness as found in a similar provision in that province's *Freedom of Information and Protection of Privacy Act*:

> *[49] By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable"*

> *does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.*
>
> *[50] The reasonableness standard in s. 30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.*

[14] I agree with the B.C. Commissioner's comments on "reasonableness" in the context of the protection of personal information. Regardless of whether the privacy provisions of the *ATIPPA* were in force at the time of the particular breach which is the subject of this investigation, I would expect that the Public Health Laboratory, as well as DHCS (and Eastern Health for their role in providing I.T. services to the PHL) would wish to be judged on a standard of reasonableness, so that is the approach I intend to take with my comments.

[15] The B.C. Commissioner also commented at paragraph 52 of the same Investigation Report about the need to consider the sensitivity of the information when determining the need for security:

> *[52] The sensitivity of the personal information at stake is a commonly cited, and important, consideration. For example, a computer disk or paper file containing the names of a local government's employees who are scheduled to attend a conference or take upcoming vacation does not call for the same protective measures as a disk containing the medical files of those employees.*

I agree with the B.C. Commissioner on this subject as well, because it is impossible to assess the reasonableness of a privacy protection measure without considering the sensitivity of the information to be protected. Generally speaking, the PHL, in holding records such as HIV and other sensitive test results, can be considered to be in possession of some of the most sensitive personal information available.

[16] Section 2(o) of the *ATIPPA* defines personal information, and also provides specific examples:

2. In this Act

> *(o) "personal information" means recorded information about an identifiable individual, including*
>
> […]
>
> *(vi) information about the individual's health care status or history, including a physical or mental disability*
>
> […]

It is clear to me that the information disclosed in this privacy breach meets the definition of personal information in the *ATIPPA*.

[17] DHCS indicated that it used guidelines developed by the Office of the Privacy Commissioner of Canada in responding to the privacy breach. That policy contains four key steps: 1) breach containment and preliminary assessment; 2) evaluation of the risks associated with the breach; 3) notification; and 4) prevention. These "key steps" are similar to those set out in the policies of other jurisdictions across the country, as well as a document produced in January 2008 by this province's Department of Justice ATIPP Office entitled "Key Steps When Responding to a Privacy Breach." This latter set of guidelines had not yet been produced when the breach occurred, but the key steps are essentially the same. It is clear that DHCS correctly identified and applied the appropriate framework within which to approach the situation. I will now review each of the four steps identified above with a view to commenting on the effectiveness of the approach taken by DHCS and the other parties involved.

[18] As noted above, the first step for a public body to take when it is made aware of a privacy breach is to contain the breach. Fortunately, the New York company acted as somewhat of a white knight in this case by directly telephoning the Consultant while the breach was ongoing and instructing her how to discontinue the sharing of her files over the internet. As such, the breach was essentially contained as soon as possible after the Consultant became aware of it. The Consultant then acted correctly by immediately telephoning senior management at PHL to advise them what had happened.

[19] The next step involves evaluating the risk. The guidelines from the Privacy Commissioner of Canada which were used by DHCS list several considerations here. The first is whether or not the breach involves personal information. There are several factors under this heading, including whether the information is in fact personal information; whether it can be accessed (it may be encrypted or otherwise inaccessible); how sensitive is the information and in what context is the information presented (it could be a list of names signed up for a soccer tournament, or it could be highly sensitive medical information); how can the information be used to harm the affected individuals (that is, is identify theft or other fraud a potential risk? What about embarrassment or humiliation?).

[20] Further considerations in evaluating the risk include determining the cause and extent of the breach, which can indicate whether the information was lost or stolen, or whether the breach was deliberate or accidental, whether the information can be recovered, or whether the breach was due to a systemic problem or an isolated incident. The process of evaluating the risk also includes identifying who and how many people may have been affected by the breach, as well as assessing the foreseeable harm which might come from the breach.

[21] In this case, the team of DHCS, PHL and OCIO analysed the 375 files known to have been accessed by outside parties through Limewire. They determined that the files held patient information on 151 individuals which contained some or all of the following elements: initials, name, gender, MCP number, physician name, lab test and result. The team further determined that the files did not contain data such as dates of birth, home or business addresses of patients or other contact information. This Office was advised by DHCS that the 375 files contained information used by the Consultant prior to her retirement as an employee of PHL, however none of it was relevant to her work as a Consultant.

[22] The team's analysis showed that of the 151 individuals, 47 were named in combination with several pieces of data pertaining to their health status. For example, 18 of these 47 individuals were listed in a file name with the acronym HIV in it, which would appear to be a list of individuals who were tested for HIV. The first and last names, gender, age, and hospital or clinic

location of the individuals were contained in that file. The other 29 (of 47) individuals were listed in other files containing test names and clear or implied test results.

[23] The remaining 104 (of 151) individuals listed were identified, but the information was not as extensive. For example, none of these 104 individuals were listed in conjunction with their age, MCP number or hospital/clinic location, and only one of the 104 was listed with their physician's last name. Most were identified by their full name, but some were only identified by initials or first name.

[24] DHCS did not appear to consider notification in 10 cases where only initials and test results or first names and test results were the only data involved. DHCS did not explicitly state why these names were not considered for notification, but presumably accurate identification of the individuals would make notification difficult if not impossible, and furthermore the difficulty in identifying the individuals would make the possibility of harm close to nil.

[25] In terms of the remaining 94 (of 104) individuals, DHCS accessed the MCP database to determine what contact information was available for those whose first and last name was disclosed. The results of this exercise varied. Some individuals were deceased, or were not registered with MCP, while others shared the same name as multiple other individuals on the MCP database. In other words, if the name John Smith and a test result was the only information relating to that individual, the MCP database may have turned up multiple John Smiths, with no immediate way of determining which John Smith received that particular test. In these instances, DHCS determined that it could not reasonably determine the correct contact information for these individuals without creating a secondary breach of privacy, so it was decided that they would not be contacted.

[26] Finally, DHCS concluded that even in instances where one of the names matched a name in the MCP database that even that information may not be accurate. DHCS was concerned that there may be a variation in the way a name was recorded for the test purpose compared to how the name is entered on the MCP database. Using the name John William Smith again to illustrate, DHCS was concerned that variations might include John Smith, John W. Smith, Jack

Smith, Johnny William Smith, etc. DHCS decided not to contact the 94 individuals because identifying them would be problematic, and the likelihood of error and further privacy impacts, weighed against the risk of identification from the information which was already disclosed during the breach, would not justify attempting to contact these individuals.

[27] Based on the sensitivity of the information and the risks and benefits of contacting the affected individuals, DHCS then proceeded on 28 November 2007 with notification to the 47 individual patients (as well as two employees whose personal information was also exposed during the breach) for a total of 49. Letters were sent to the two employees notifying them of the breach. In relation to the 47 patients DHCS intended to notify, DHCS provided the following breakdown as of 4 December 2007:

> *47 identifiable patients:*
>
> *38 letters have been sent out*
> *3 deceased*
> *1 child who has since been adopted*
> *2 left province (no forwarding address)*
> *2 no record of ever having been registered with MCP*
> *1 not enough information to determine address*

[28] This further review, then, reduced the number of individual patients to be notified down to 38. In its letter to this Office dated 4 December 2007, DHCS stated that the letters to the 38 individuals

> *…were delivered in a number of ways to ensure that no further breach of privacy, directly or indirectly, could take place. Patients listed in the* [*file with HIV in the filename*] *were initially contacted by telephone by a nurse from the HIV Clinic who explained the nature of the information that had been released and asked how they would like to receive the written notification. Most opted for delivery through the HIV Clinic. Other notification letters were sent by special registered mail where the recipient is required to show proof of identification prior to receiving the letter. One case involved using the services of the Office of the High Sheriff and another used a private process server. The two employees were initially contacted by telephone and then received the written notification from a courier.*

[29] DHCS updated this Office on 8 February 2008 to state that four of the 40 letters sent (38 patients, two employees) which were sent by special registered mail were returned as undeliverable, and DHCS does not have any other contact information for these individuals.

[30] The fourth step is prevention, which again, is common to policies across the country relating to the steps to take in responding to a privacy breach. In my view, this is the most significant part of this matter, not only in understanding how this breach occurred, but also in reviewing current and planned policies and practices which are meant to prevent this type of breach from occurring in the future. In order to consider the steps taken to prevent future breaches of this kind, I will briefly review some of the major contributing factors which allowed this breach to happen, or which could have helped prevent it, in conjunction with the subsequent preventative measures taken or proposed.

Contractual Employees and Privacy

[31] One of the factors which allowed this breach to occur began with the decision by PHL to place the Consultant (who had recently retired as an employee) on a contract to provide services to PHL. In reviewing this contract, it is clear that no provision was made for the protection of personal information held by the Consultant on the desktop computer which was issued to her in order to perform her contractual duties outside the workplace. The status of a contracting entity, whether individual or corporate, is defined in the *ATIPPA* as follows:

> *2(e) "employee", in relation to a public body, includes a person retained under a contract to perform services for the public body;*

[32] Clearly, then, the *ATIPPA* is constituted such that there is no distinction to be made between an employee of a public body and a person retained under a contract to perform services for a public body. The contractor and the employee share the same obligations in terms of privacy and access to information, and the public body is also obliged to ensure that both the employee and the contractor are in compliance with the *ATIPPA*. It is expected that staff and management of a public body who handle personal information will have received training and will have a clear understanding of their obligations in relation to the protection of privacy. Privacy protection

must be built into the contractual language when hiring contractors who will be handling personal information so that the public body can satisfy itself that contractual employees are aware of and understand their obligations under the *ATIPPA*, and also that contractors understand that it is an explicit condition of their employment that they are required to abide by the *ATIPPA*. In some cases, this contractual language may be more specific or elaborate where the work to be performed is directly related to the handling of personal information. In other cases, the contractual language may be of a more general nature if the handling of personal information is not expected to be a significant part of the anticipated duties. Contractual employees may require privacy training, depending on the nature of their work. The end result should be that contractors should not be a "weak link" within a public body when it comes to privacy. The public body should operate at a high level of privacy compliance, and must ensure that any work performed for the public body on a contractual basis is done within a comparable degree of privacy compliance.

[33] In this particular case, the contract was quite basic and short, simply outlining the duration of the contract, the rate of pay, the persons to whom the contractor is to report, and a brief reference to the nature of her work. The contract was signed by the Consultant and the Director of the Public Health Laboratory. The contract contained no reference to the *ATIPPA* in relation to the collection, use and disclosure of personal information or reasonable security arrangements which must be in place to protect any personal information in the contractor's possession.

[34] This Office has been advised by DHCS that PHL did not view the engagement of the Consultant who was involved in this privacy breach as the engagement of an external consultant, because the individual "was a long term, devoted employee of the lab who agreed to assist … on an as needed basis" after retirement. While I can appreciate the esteem within which the lab held this individual, it is clear that this individual had retired from regular employment, and was under contract to perform certain duties while in retirement. Despite many years of association with PHL, this individual was clearly acting in the capacity of a contractor at the time that a significant privacy breach occurred. Consistently applied procedural safeguards, grounded in policy and based on the *ATIPPA* and/or other applicable legislation are reasonable measures to

protect privacy. One element of such policy and procedure would be the insertion within any contractual language of appropriately detailed privacy obligations.

[35] This Office has been advised that the Department of Justice and OCIO has recently developed a new template for insertion in contracts which involve the handling of personal information. This Office has also been advised that "all government contracts with external consultants and contractors, which contemplate access to personal information, should be reviewed by one of the solicitors at the Department of Justice." This recommendation comes from the 1993 revision of the Treasury Board Consultant Guidelines, which remain in place. Given that the new privacy template has only been developed following the privacy breach which is the subject of this report, review of the Consultant's contract by the Department of Justice may not have made a difference in this case. However, now that the privacy template has been developed, it is essential that PHL follow the Treasury Board Guidelines in this respect in future, and furthermore that it use the new privacy template whenever a contractor is to be hired.

[36] If the Consultant had been required to review and agree to stringent privacy protocols in order to accept employment on a contractual basis following her retirement, it would have been an opportunity for PHL and the Consultant to consider more fully the potential privacy implications of her work. It may, for example, have served to remind both parties to ensure that all personal information was erased from her computer before removing it from PHL, and to enlist the IT experts at Eastern Health to perform this task. This brings us to the next factor to be considered.

Removal of Desktop Computer from Work Site

[37] Several months before the privacy breach occurred, permission was given by PHL management for the Consultant to remove a desktop computer from the premises of the Public Health Laboratory, which was the same computer she had used prior to her retirement. According to information provided by Eastern Health, Eastern Health IT staff were instructed by PHL management to transfer the information on the Consultant's computer to the computer of the person who would be replacing the Consultant upon that person's retirement. As noted

above, Eastern Health provides IT support services to PHL. Eastern Health says, however, that its IT personnel did not remove the information from the Consultant's computer, because "PHL management wanted to give the employee [who became the Consultant subsequent to retirement] time to review all files prior to retiring." Eastern Health said that its IT personnel were not aware of the plan to remove the computer from the workplace, they were not asked to "clean" the computer of all data prior to its removal, nor were they aware of efforts made to remove the data prior to it being taken home by the Consultant. Eastern Health stated that "if requested, Eastern Health's IT staff would have ensured that all data was removed from the computer prior to it leaving PHL."

[38] According to DHCS, PHL policies and procedures in relation to this issue were reviewed and amended following the breach. This resulted in specific policies prohibiting the removal of any files containing patient information from the physically secure environment of the PHL, and also prohibiting the removal of a desktop or laptop computer containing personal information from the PHL premises. DHCS later provided more specific information on these new policies, as outlined later in this Report, in the section entitled, "Policies and Procedures."

Training

[39] Parts I, II, III and V of the *ATIPPA* came into force in January of 2005. The privacy provisions, contained in Part IV were not proclaimed into law at that time. The stated purpose of the delay was outlined in the House of Assembly on 13 December 2004 by the Honourable Tom Marshall, who served as Minister of Justice and Attorney General at the time:

> *Part 4 of the act dealing with privacy will be delayed, as was originally intended, and as has been the plan from the outset, for one year to allow all bodies covered by the act to educate and equip themselves to adequately implement the privacy protection provisions of the act.*

[40] Minister Marshall provided a further update in *The Telegram* on 29 March 2006, when he stated that the privacy provisions of the *ATIPPA* had not yet been implemented, but that this would happen following the provision of adequate training for public bodies:

> *We're going to commence a comprehensive training program for all public bodies, right across government, so that they will know how to comply with the spirit and intent of the legislation.*

[41] Despite this publicly stated goal by the Minster responsible for the *ATIPPA*, and the three year delay in implementing the privacy provisions to allow for education and training within public bodies about those provisions, DHCS has acknowledged to this Office that neither PHL staff nor management had attended any privacy training sessions with respect to the *ATIPPA*. DHCS noted in its 8 February 2008 submission to this Office that PHL staff had not been offered any training until recently with respect to privacy. This position was modified somewhat through later correspondence initiated by this Office. It is apparent from this investigation that by mid 2007 DHCS and the Department of Justice were actively engaged in discussing and then planning privacy training for specific agencies within the health sector, however, none were yet planned or scheduled for PHL at the time of the breach. Furthermore, I have no information to the effect that any such training was being considered for PHL prior to the privacy breach.

[42] In reply to questions about privacy training, DHCS indicated to this Office that the professional and educational backgrounds of staff at PHL would likely have included course curricula and seminar content which would highlight privacy and confidentiality issues respecting laboratory data. DHCS forwarded to this Office a copy of the Code of Professional Conduct of the Canadian Society of Medical Laboratory Science, of which all laboratory technicians at PHL are members. That Code requires that "medical laboratory professionals shall protect the confidentiality of all patient information." DHCS also indicated that PHL operates in a secure environment where privacy and confidentiality are paramount, and that these values are enforced through professional codes of ethics, professional certifying bodies, and employee oaths of confidentiality.

[43] DHCS indicated in its correspondence of 22 May 2008 that two meetings were held at PHL in the days following the breach, on 22 November and 26 November 2008 in which staff attendance was compulsory. The purpose of these sessions was to discuss security and

confidentiality protocols. A Memorandum on policy and procedure was distributed at the second meeting (see below for more on the Memorandum).

[44] DHCS noted that training is planned for the near future, specifically with reference to the *Personal Health Information Act (PHIA)*, which was passed in the Spring 2008 session of the House of Assembly. A news release from DHCS on 20 May 2008 indicates that proclamation into law of the *PHIA* is targeted for 18 months time in order to allow for education and awareness within the health system and the general public. Once the *PHIA* comes into effect, it will govern the collection, use and disclosure of personal health information, and will therefore replace the *ATIPPA* in applying to that particular category of personal information. Until that time, the *ATIPPA* continues to govern the collection, use and disclosure of personal information (including information relating to a person's health). DHCS indicated that this upcoming training in privacy and confidentiality would be done in collaboration with the Newfoundland and Labrador Centre for Health Information, and would include on-site as well as on-line components, with the goal of ensuring that all staff involved in the collection, use and disclosure of personal health information receive the training.

[45] This proposed level of training, if it is properly designed and carried out, should serve as an important preventative measure to help DHCS avoid future privacy breaches. I must note, however, that DHCS appears to have focused on preparing for the *PHIA*, while failing to arrange for sufficient training in relation to the privacy provisions of the *ATIPPA*, which are now in force. While the *PHIA* is different in many ways from the *ATIPPA*, any aspects of training which might focus on the prevention of privacy breaches would likely be very similar.

[46] DHCS has a responsibility to protect the privacy of patients who have entrusted their personal information to PHL. The privacy provisions of the *ATIPPA* simply codify that responsibility, making it explicit and specific. Adequate training of staff and management is an essential component of any reasonable level of privacy protection for patients, and specific training which might flow from or result in the development of new policies and procedures to ensure compliance with the *ATIPPA* may have helped to prevent this breach. DHCS has not specified the time frame for its upcoming training, but I would recommend that it be done in the

very near future in order to arm management and staff with the knowledge to help prevent future privacy breaches.

Information Security (Installation and Use of Limewire / File Sharing Software)

[47] There is no evidence that there were specific policies in place at the time of the breach, whether at Eastern Health, PHL or DHCS, in relation to the use or installation of file sharing software on computers owned or controlled by those entities. I will not comment in detail on the specific hardware and software installed by Eastern Health IM&T (Information Management and Technology) and used by PHL in relation to firewalls, passwords, encryption, etc, except to say that DHCS and Eastern Health need to ensure that a reasonable level of security for its electronic data is in place. DHCS, PHL and Eastern Health must work together to determine the required level of security for electronic data in the custody of PHL. Eastern Health has provided some information on the types of technical security it had in place previous to this privacy breach, as well as the additional security which it plans to initiate. Eastern Health indicated in particular that it was looking at upgrading and improving security for laptop computers with encryption and other measures following the breach. Although encryption would not have prevented this particular breach because it was unknowingly initiated by the computer's approved operator, any information security improvements undertaken by Eastern Health are to be encouraged.

[48] I am pleased to note that PHL has participated in a very in-depth and comprehensive IT Security Framework review conducted by an outside agency. That review recommends specific actions and policy initiatives with a view to protecting the sensitive information which is in the care of PHL. On the basis of that review, hopefully augmented by this Report, DHCS and PHL should have a much clearer picture of the further reasonable steps which it should take in order to protect the personal information in its possession.

[49] This Office was provided with a copy of Eastern Health's Information Management & Technology Policy and Procedure entitled "Personal Computer Systems" as part of DHCS's submission on 8 February 2008. Despite my difficulty in obtaining clear communication from DHCS on the status of its policies and procedures for electronic records at PHL (which will be

covered in the next section) it is clear that Eastern Health's policy places responsibility for protection of the information stored on a personal computer in the hands of the user. Procedure 1.1 states that "Users of Personal Computers systems [sic] are responsible for the security and confidentiality of all information contained on the system's hard disk or on any backups, such as floppy disk or magnetic tape." Furthermore, the Introduction section of the Policy states that

> *All third party software contained on a Personal Computer must be a legally licensed copy. All Users are responsible for the legality of their system software. Any user wishing to install software not purchased by the Health Care Corporation of St. John's* [now Eastern Health] *must contact IM&T and show proof of ownership prior to software installation. All software will be checked to ensure it is virus free prior to being installed.*

[50] Based on this Eastern Health policy (and PHL says that it follows Eastern Health policies and procedures in relation to IT), it appears that the Consultant was in violation when she installed Limewire on her computer without first checking with IM&T. I am unaware as to whether this particular policy has been updated or replaced, but it seems to allow quite a wide latitude for employees to install any program on their work computers as long as they can prove it is licensed and there are no viruses. Typically, policies such as this one would be concerned with copyright and viruses, rather than information security and privacy. I would expect that this policy would need to be revisited in light of PHL's experience with Limewire. I have not been advised of any change in that policy since its receipt at this Office. Although the Eastern Health policies and procedures which were provided to me were not numbered, dated, or signed for approval, they appear to be appended to the PHL policies which were provided. The above noted Policy in particular appears to be referenced as a procedure associated with PHL's Policy "PHL IM-004." I was unable to determine whether Policy "PHL IM-004" is a draft or approved policy. This will be addressed further in the next section.

[51] My final comment on this subject is that policies are not effective if they are not monitored and followed. Simply putting all of the responsibility in the hands of the user, as the above policy does, amounts to very little in terms of protecting personal information. As noted earlier, section 36 of the *ATIPPA* places the responsibility on the head of the public body for provision of reasonable security to prevent privacy breaches. It is unknown whether employees were

receiving ongoing training and instruction about their responsibilities in relation to handling personal information in electronic format, or whether most employees would even have been aware of this set of policies and procedures. DHCS and PHL, through Eastern Health, must recognize the pace at which technological developments are moving.

[52] Policies which simply tell users they are responsible for the information they handle are no longer sufficient. Clearly, no one anticipated Limewire when these policies and procedures were drafted. The ubiquity of such programs now means that technical barriers to prevent their installation and use in the workplace must be strongly considered. It is not enough to place all of the responsibility in the hands of individuals, because technology has become complex enough and changes so quickly that all individual employees cannot be expected to act as their own information security experts.

[53] Furthermore, policies and procedures in relation to the security of personal information stored on electronic media must be regularly reviewed and updated. A formal schedule for such reviews on an ongoing basis should be developed by Eastern Health and DHCS. Perhaps they could work with the OCIO to develop best practices and to ensure that the most up-to-date security provisions are in place. The very comprehensive review of PHL IT Security which I referenced above appears to be an excellent resource, and I would hope that it is utilized to its maximum potential.

Policies and Procedures (Electronic Records: Information Handling, Retention & Destruction of Records, etc.)

[54] Good records retention and destruction policies and practices are essential, not only to information management, but to privacy as well as access to information. A question which needs to be asked, from a prevention point of view, is whether such records need to be retained, and whether they were maintained in compliance with or in contravention of PHL's own records retention policy. DHCS has clearly indicated to this Office that none of the information disclosed in the privacy breach was relevant to the Consultant's work at the time of the privacy breach. It had, however, been relevant prior to her retirement as an employee.

[55] DHCS provided a copy of its records retention policy, "PHL D-0008 Document and Records Retention Procedure." The stated purpose of the policy is "to provide guidance to employees on the management of confidential patient information and materials." The policy states that "in addition to internal safeguards, the PHL complies with the confidentiality and security policies of the Information Management and Technology Department (IM&T), Eastern Health." The paragraph in the policy entitled "Responsibility" lists PHL management and employees, and Eastern Health IM&T employees. It appears, then, that the policy is meant to be followed by both Eastern Health IM&T employees as well as PHL management and employees. Furthermore, the policy itself refers, under "Procedure" to policies originating with Eastern Health. In particular, it states that "the same level of confidentiality and security applies to both manually written and electronic records."

[56] Upon further inquiry during this investigation, however, DHCS has advised that the policy "was, at the time of the breach, and remains a draft document." The policy sets up various categories of records with storage time and location. When asked which category the records involved in the privacy breach fell into, DHCS advised that they "… would not fall into any of the categories contained in the draft document. The lab considers them to be electronic records. The lab follows the policies, procedures and risk management schedules of Eastern Health for electronic records." It therefore appears that DHCS forwarded to this Office a policy which is neither in force, nor even applies to the records at issue.

[57] In a follow-up e-mail dated 6 May 2008, DHCS was asked to "… provide copies of these policies, procedures, and retention/destruction schedules for electronic records" if there were any in addition to those already provided in DHCS's submission of 8 February 2008. On 22 May 2008 DHCS advised that this Office had "…already been provided with a copy of any policies and procedures that existed at the time of the breach with respect to retention and destruction schedules for electronic records." I note that we were only provided with two PHL policies with DHCS's 8 February 2008 submission, one being "PHL D-0008 Document and Records Retention Procedure," which we were later informed is a draft document and does not apply to electronic records. I am forced to draw the conclusion that PHL has no policies regarding the

retention and destruction of electronic records. (The other PHL policy provided at that time was PHL IM-004, referenced above in the section on Policies and Procedures, and again below).

[58] Furthermore, DHCS had been asked for policies and procedures ***and*** retention/destruction schedules for electronic records. DHCS, in its 22 May 2008 correspondence only referenced that it had already provided policies and procedures regarding retention and destruction schedules. DHCS did not reference whether there were other policies or procedures regarding electronic records. The only other policy in relation to electronic records was provided to this Office with DHCS's submission of 8 February 2008. DHCS was asked in an e-mail dated 6 May 2008 to "…provide copies of all of the policies, procedures and schedules which were reviewed [subsequent to the breach], indicating which are draft, which are in force and the date they came into force, and identifying particular changes which were made to those policies, procedures and schedules following the privacy breach?" In its response of 22 May 2008, DHCS did not reference the only other Policy which it had provided with its February 2008 submission – Policy PHL IM-004. Therefore, I am unable to state whether this policy is in force and if so what date it came into force, whether it is a draft policy like PHL D-0008, or whether it was amended subsequent to the privacy breach. However, DHCS did provide, with its correspondence on 22 May 2008, a copy of a Memorandum dated 26 November 2007 from the PHL Operations Manager to all PHL employees, in which recipients are advised that "effective immediately I would like to inform you of some changes to our policy and procedures and to reiterate some of our current practices." The changes outlined in the Memorandum were:

- *Our in-house policy pertaining to discarding of confidential information has changed. All papers and documents containing patient information and other confidential information will be shredded on site instead of being placed into the locked recycling bins as per current practice.*
- *No files containing patient information can be removed from the physically secure environment of the PHL.*
- *For sharing or analyzing research related data with stake holders, encrypted memory sticks must be used with coded patient information.*
- *No paper reports containing identifiable patient information can be left unattended at the PHL.*
- *Mandatory use of additional locking cabinets.*

[59] It is unclear which "in-house policy" is being referred to in the first bullet point above, or whether all of the points are changes to pre-existing policies or whether they are all new. If the reference to the "in-house policy" is a reference to Policy PHL D-008, I note again that DHCS has advised that this policy is a draft policy, and is not in force.

[60] In addition to the other information provided by DHCS in its 22 May 2008 correspondence, DHCS included a draft copy of Eastern Health's new draft Record Retention & Destruction policy. I realize that it is a new draft, and I will therefore not comment extensively on it, except to encourage PHL, before simply adopting Eastern Health's policy, to ensure that the type of records which were involved in the privacy breach would be adequately covered. For example, I note that the records involved in the breach were no longer needed by the Consultant, and there is no indication that they were to be used again in the future. The records did not appear to be original patient records, but rather composed largely of statistical tables containing patient names and other identifying information. PHL should ensure that such records are either stored appropriately for a designated period of time or destroyed once the purpose for which they were compiled has ceased, and that appropriate policies are in place to guide such decisions.

[61] DHCS also provided, with its 22 May 2008 correspondence, a copy of a Pledge of Confidentiality, which it says that all PHL employees have signed. A person signing the pledge agrees that he or she has read and will abide by the Confidentiality Policy of the Health Care Corporation of St. John's (now operating as Eastern Health). The Confidentiality Policy attached refers to the confidentiality of patient information being a legislated requirement under the *Hospitals Act*. I note that the *Hospitals Act* was repealed on 1 April 2008. While it is positive that employees are required to read and abide by this policy, it should be updated to reflect current legislative standards, including the *ATIPPA*, which is presently the applicable privacy law, and also the *PHIA* when it comes into force.

[62] Despite the questions and follow-up questions posed by this Office, I still do not have a clear picture as to the policies and procedures which are in place to govern how electronic records are managed, retained or destroyed at the Public Health Laboratory. Given the time that has elapsed since this investigation was requested, however, I have decided not to ask for further

clarification. I will simply say that a comprehensive set of formally approved and up to date policies and procedures governing management, retention and destruction of electronic records is a key aspect of any public body's effort to protect personal information, and in my view it is an essential task for DHCS and PHL.

Roles and Responsibilities

[63] Who makes the rules, and who follows whose rules? One of the things we sought to clarify in this Report is who is actually responsible for the electronic information held by PHL. We began by attempting to determine the formal protocols which one would expect to exist governing the relationship between PHL and Eastern Health. In response to this issue, DHCS provided me with a letter from the Director of PHL, who explained that

> *There is no formal MOU* [*Memorandum of Understanding*] *between PHL and Eastern Health concerning the provision of IT services. This is attributable to the operational relationship between the two which dates back to several decades when PHL functioned as part of the old General Hospital. This relationship continued on when General Hospital moved to its present location in the mid 1970s as Health Care Corporation. PHL introduced the Meditech lab information system in consultation and conjunction with Eastern Health IT in 2002, and the provision of the required IT services by EH* [*Eastern Health*] *was assumed and PHL followed IT protocols and guidelines of EH.*

[64] The issue of the status of PHL was, however, subject to some correspondence between DHCS, PHL and Eastern Health (then the Health Care Corporation) in 2002 and 2003 when an MOU regarding the administration of employees of the PHL was drafted. Unfortunately, it appears that nothing specific appears to have been developed which would formalize the responsibility for electronic records at PHL. This was made quite apparent from the views expressed by Eastern Health and DHCS in DHCS's submission of 8 February 2008. By way of explanation, DHCS's submission was the result of a series of questions posed by this Office. DHCS asked Eastern Health to respond to some of the questions which it deemed appropriate to Eastern Health's responsibility or jurisdiction. As part of its submission, DHCS offered the following comments:

- *… PHL follows the IM/IT policies and procedures of Eastern Health.*
- *Eastern Health is responsible for establishing privacy and security protocols respecting electronic data at the PHL.*

At the same time, Eastern Health's related comments, which were appended to DHCS's submission, are as follows:

- *Eastern Health is responsible for the electronic information in PHL's Meditech Laboratory Information System.*
- *Eastern Health is not aware of PHL's data retention / destruction policies or schedules. This is the responsibility of PHL management.*

[65] This appears to be a key point, and one which bears emphasis in this Report. DHCS has stated that "Eastern Health is responsible for establishing privacy and security protocols respecting electronic data at the PHL," while Eastern Health says that "Eastern Health is not aware of PHL's data retention and destruction policies or schedules. This is the responsibility of PHL management." There appears to be a significant disconnect here among these organizations as to whose policies should be followed, who is responsible for developing such policies, and which organizations are governed by the policies. Data retention and destruction policies are an essential element of privacy protection. They cannot exist in isolation from other privacy protocols. Clearly, this privacy breach would never have occurred if the records stored on the Consultant's computer had been erased in compliance with an appropriate records retention and destruction schedule, because those records were no longer needed by the Consultant.

[66] Eastern Health commented as follows in relation to the computer involved in the breach:

> *Eastern Health provides technical support for the PHL Meditech L.I.S. system and their desktop computers. While providing this service our staff follows the policies and procedures of Eastern Health unless directed otherwise by PHL management.*
>
> *With respect to the computer involved in the breach, Eastern Health IT staff followed instructions given by PHL management which included transferring the information on the computer to a new internal computer of the person replacing the individual currently using the device. Eastern Health IT staff were not asked to clean the computer, PHL management wanted to give the employee time to*

> *review all files prior to retiring. Since Eastern Health was not aware that this computer was being removed from the workplace and was not asked to clean the device prior to removal we are not aware of the efforts made to remove the data prior to it being taken home by the consultant. If requested, Eastern Health's IT staff would have ensured that all data was removed from the computer prior to it leaving PHL.*

[67] There is a difference between PHL adopting and following Eastern Health policies and procedures, and being responsible for its own activities. I can accept that PHL has adopted Eastern Health policies and procedures. This does not mean, however, that Eastern Health is responsible for the activities of PHL in relation to activities governed by those policies. Returning to the comments of the British Columbia Information and Privacy Commissioner about letting the sensitivity of the information be one of the determinants of the most reasonable level of security, it is clear that PHL is the entity which is best able to assess the sensitivity of the data in its possession. Eastern Health IT is not in a position to analyze that data in order to determine what level of security must be utilized, nor should it be acting in that role. PHL can adopt the policies and procedures of Eastern Health, and Eastern Health can continue to provide IT services to PHL, but PHL is ultimately responsible for the information in its possession. If Eastern Health IT is not aware that a contractual employee will be removing a computer from the workplace, it can not be expected to follow any policies or procedures which may govern such instances.

[68] It appears that Eastern Health sees itself in more of a worker role when it comes to IT. They will come in and do a specific job (desktop computers and the Meditech system), and they will do that job according to Eastern Health policies and procedures unless directed otherwise by PHL management. The statement by Eastern Health (noted earlier) that it was unaware that the Consultant's computer was being removed from the workplace, is consistent with Eastern Health's view of its role as simply following directions. At the same time, DHCS and PHL seem to be of the view that Eastern Health is much more than a worker. DHCS has concluded that Eastern Health is responsible for establishing privacy and security protocols respecting electronic data at the PHL. Clear roles and responsibilities must be developed among these parties. Without such clear delineation, there is a real risk that certain aspects of privacy protection will continue to slip through the cracks, despite the best intentions of the parties involved.

Privacy Impact Assessments

[69] DHCS indicated in its response that no privacy impact assessments were completed in relation to the Consultant's project. A privacy impact assessment is a tool which can be used to assess the privacy compliance of a particular project. The Department of Justice ATIPP Office has created an excellent resource, the ATIPP Privacy Manual (available online), which can assist public bodies in conducting privacy impact assessments. Once again, this is another preventative measure which public bodies should undertake in relation to the collection, use or disclosure of personal information. Although the ATIPP Privacy Manual was not published until January 2008, I must take this opportunity to highlight such an important preventative measure. Recognizing that PHL did not have the benefit of that Manual at the time, I encourage DHCS on a go-forward basis to work with the Department of Justice ATIPP Office to ensure that PHL staff and management receive sufficient training in when and how to conduct a privacy impact assessment. Additional resources on privacy impact assessments are widely available on the internet, as well as on the web site of this Office, where it is referred to as a Privacy Audit.

V CONCLUSION

[70] I want to emphasize here that this Report is not meant to be a comprehensive review of all aspects of privacy at PHL, but simply to provide an assessment and recommendations in relation to the prevention of future privacy breaches like the one which led to this Report. This Report has focused on prevention, simply because DHCS, with the assistance of OCIO and EWA, has done an excellent job in analyzing and responding to the privacy breach, including appropriate notification of affected individuals.

[71] The decision by DHCS to request our involvement has turned out to be a timely one, as the privacy provisions of the *ATIPPA* were proclaimed into force by government in January 2008. Although no violation of the privacy provisions can be said to have occurred in relation to this breach because those provisions were not in force at the time, I see this investigation and Report

as an opportunity for this Office and for DHCS, as well as public bodies across the province who are now subject to the privacy provisions of the *ATIPPA*, to help bring about a new era of privacy protection. It is my intention that reports such as this will not simply be critical where criticism is warranted, but also point out whenever possible the positive measures which have been put in place by public bodies to protect privacy. These reports can then serve a constructive purpose over and above the investigation of a particular privacy complaint – they may in some measure shine a light on outdated policies and practices which should be discontinued, and privacy-enhancing policies and practices to be emulated by public bodies. If this purpose can be accomplished to some degree with each report, then it will help accomplish one of the primary purposes of the *ATIPPA*, which is to protect the personal privacy of Newfoundlanders and Labradorians.

[72] I should note that OCIO has provided excellent cooperation to this investigation. OCIO was called upon by DHCS to take a leading role in determining the extent and cause of the privacy breach, and since that time, OCIO has been working hard to develop new policies and is working on informing all public employees about privacy and confidentiality from an IT security perspective. These initiatives are to be applauded and encouraged, and further initiatives of this kind must be undertaken within the health sector, which holds so much sensitive personal information.

[73] I wish once again to commend DHCS for inviting this Office to investigate this privacy breach, even though it occurred prior to the privacy provisions of the *ATIPPA* coming into force. This demonstrates a commitment to accountability, and shows that it is very serious about developing a high standard of privacy protection within PHL and elsewhere within DHCS.

[74] One small observation I want to make is that, from the beginning, DHCS (and government) referred to this incident as a "security" breach, and in a significant aspect it was. From my perspective, however, it was also, or primarily, a "privacy" breach. Security of information is an essential aspect of the protection of privacy, but it is not the only one. Technical and physical security measures are useless if they do not anticipate certain activities or behaviours by employees of public bodies. Privacy, then, also encompasses policies, procedures, and ongoing

education. In this case, someone removed, with permission, a computer from the network and from the secure environs of PHL. When a physical or technical safeguard has failed, leading to the unauthorized disclosure of information, we have a "security" breach, but if that disclosure includes personal information, it is also a "privacy" breach. Public bodies must begin to recognize that we are operating in a new environment now – one of privacy protection, thanks to the *ATIPPA*, and we must therefore learn to identify it as such.

[75] It is simply not adequate to state that employees have certain professional training and accreditation which covers privacy. If this were sufficient, there would be no need for privacy legislation. Management and staff of public bodies who handle or are responsible for personal information must receive appropriate privacy training. I do not accept any reason for delay in privacy training based on the perceived need to focus on the *PHIA*, which will not be in force until at least late 2009, because the *ATIPPA* is already in force, and until the *PHIA* is proclaimed, the *ATIPPA* applies to all information held by public bodies, including personal health information. In fact, the *ATIPPA* will continue to apply to some information held by public bodies in the health field even after the *PHIA* comes into force, such as various administrative records. I would expect that the type of privacy training which might have helped to prevent this privacy breach would have covered basic privacy principles which are common to both the *PHIA* and the *ATIPPA*, as well as some common sense policies and procedures. I am not suggesting that such training would necessarily have been specific enough to cover the risks of installing Limewire on a PHL computer, but rather that it would have at least served to raise awareness, and perhaps to cause management and the Consultant to think twice about removing a computer from the workplace without first ensuring that all unnecessary personal information was removed. In my opinion, training is the first and most essential step in building a culture of privacy, whereby privacy eventually becomes a paramount consideration in any activity. Privacy training and policy review must be ongoing elements of the new workplace culture. Nothing can be assumed based on employees' professional background or formal education, which may or may not be adequate depending on the individual.

[76] Longstanding informal arrangements regarding information management and information technology are no longer appropriate nor adequate for privacy protection, where clear roles and

responsibilities, and clear policies and procedures are now necessary. The same would apply to the almost informal nature of the Consultant's contract. Such contracts are no longer adequate in today's privacy environment.

[77] Training, policy development, procedural safeguards, and technical security are not guarantees against privacy breaches. In fact, there are no guarantees against privacy breaches. Breaches will happen. However, the important thing to keep in mind is that each step taken by a public body to prevent privacy breaches represents a layer of protection. Furthermore, the *ATIPPA* requires, under section 36, that reasonable steps be taken to protect privacy. Therefore, reasonable steps toward the development of these different aspects of privacy protection are not only advisable, but are now mandated by law. We are still in the early days of statutory privacy protection in this province, and therefore my approach at this stage is to be one of education and encouragement to public bodies. As time moves on, however, expectations will be greater for public bodies to have reasonable safeguards in place, and they will be held accountable through my Reports and public comments for their actions or inactions.

VI RECOMMENDATIONS

[78] In this Report, my focus has been on specific recommendations in terms of policy and practice. Based on information provided by OCIO, Eastern Health and DHCS, I am of the opinion that significant attention has been drawn to the technical security aspect of privacy protection. It is clear that the experts in that area have been consulted, but now the onus is on DHCS and PHL to follow through on that advice.

[79] Generally speaking, public bodies must collect, use and disclose personal information only as prescribed by the *ATIPPA,* and the onus is on those bodies to determine the most appropriate technologies in order to comply with the provisions of the *ATIPPA.* While I may from time to time comment on specific technologies and their application in relation to the protection of privacy, my emphasis will be on appropriate policies and practices. I take this position for two reasons. In many cases, the best technical knowledge already exists within or can easily be

obtained by various public bodies, even if the best technologies are not always in place to protect privacy. Therefore, the capability is there, and my role is to encourage its application in support of *ATIPPA* compliance. Secondly, it is my hope that public bodies will be able to consult my Reports in support of the development of best practices for privacy protection. For that reason, I will focus more on the legislation, and on policy and procedure, which should remain relevant well into the future, rather than on particular technologies which are evolving as quickly as others become obsolete.

[80] While there are other specific suggestions made in this Report, I will conclude with several specific recommendations:

1) DHCS and PHL should ensure that any contractors (regardless of whether or not they are former employees) be required to sign a contract containing appropriate privacy language if the contractor is expected to access personal information. DHCS and PHL should work with the Department of Justice to ensure that appropriate privacy language is part of the contract.

2) The status of PHL in relation to DHCS and Eastern Health should be reviewed and clarified. Ensure that areas of responsibility are clearly detailed between both parties, including appropriate policies and procedures governing the management of electronic information and the protection of privacy. These should be set out in formal terms between Eastern Health and DHCS. All such policies and procedures, once established, should be reviewed at regular, specific intervals.

3) Privacy Impact Assessments should be completed where appropriate for new and ongoing PHL activities involving access to personal information. DHCS may wish to work with the ATIPP Coordinating Office of the Department of Justice to help introduce this practice to PHL.

4) DHCS should proceed at its earliest opportunity to plan and arrange privacy training for all staff and management at PHL. Training should be revisited on an ongoing basis as required, coincident with the introduction of new staff, or new projects, policies and procedures.

5) DHCS should work with PHL and Eastern Health to ensure appropriate implementation of the recommendations of the IT Security Framework Review conducted by an outside party following the privacy breach.

[81] The Department is requested to please respond to these recommendations within 15 days of receiving this Report.

[82] Dated at St. John's, in the Province of Newfoundland and Labrador, this 25th day of June, 2008.

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