July 23, 2008 **P-2008-002**

NEWFOUNDLAND AND LABRADOR

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

REPORT P-2008-002

Eastern School District

Summary: On 21 February 2008 Eastern School District ("ESD") contacted this Office to advise that four laptop computers had been stolen from ESD offices. Information on one of the laptops consisted of personal information including the names, addresses, MCP numbers, contact and bussing information of over 28,000 school children. ESD asked the Commissioner to investigate. The Commissioner found that sections 36 and 39 of the *Access to Information and Protection of Privacy Act* (*ATIPPA*) had been breached. The Commissioner noted that section 36 of the *ATIPPA* required public bodies to make "reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal." ESD failed to provide such reasonable security measures and this led to the unauthorized disclosure of personal information, contrary to section 39 of the *ATIPPA*. He concluded that a multi-layered approach to protection of personal information was necessary. This includes administrative, physical and technological safeguards. The Commissioner noted that while policies and directives with respect to safeguarding information stored on mobile devices were lacking at the time of the breach, such policies are now in active development by ESD. The Commissioner was satisfied with the physical safeguards employed by ESD both prior to and since the breach. Finally, the Commissioner found that encryption was the required industry standard with respect to technological safeguards. At the time of the breach, the laptops were protected by passwords only. This was not a "reasonable security arrangement" in accordance with section 36. Since the breach ESD has installed BIOS, hard drive and power-on passwords and an encrypted drive (where personal information must be stored) on all ESD office laptops. The Commissioner concluded that these measures are in keeping with section 36. The Commissioner also recommended that

ESD and the Department of Education develop and assign random unique identifiers to students to replace the use of MCP numbers.

Statutes Cited: *Access to Information and Protection of Privacy Act*, S.N.L. 2002 c. A-1.1, as am., ss 32, 36, 38 and 39, *Schools Act, 1997*, S.N.L. 1997 c. S-12.2, as am., *Medical Care Insurance Act,1999*, S.N.L.1999 c. M-5.1, as am., *Personal Information Protection and Electronic Documents Act* S.C. 2000 c. 5, as am.

Authorities Cited: Newfoundland and Labrador OIPC Report P-2008-001; Ontario OIPC Order HO-004; British Columbia OIPC Reports F07-01 and F08-02; Alberta OIPC Investigation Report P2006-IR-005; Office of the Privacy Commissioner of Canada *Annual Report to Parliament 2007*

Other Resources: *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/

http://www.ico.gov.uk/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx

http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23recon-1_e.asp#Related

www.microsoft.com/smallbusiness/resources/technology/security/how-to-protect-your-laptop-from-thieves.aspx

www.microsoft.com/uk/smallbusiness/technology-in-business/security/protect-your-sensitive-documents.mspx

http://www.microsoft.com/uk/smallbusiness/technology-in-

business/security/guard-against-theft.mspx

http://labmice.techtarget.com/articles/laptopsecurity.htm

www.scambusters.org/laptop.html

http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf

http://www.ocio.gov.nl.ca

I BACKGROUND

[1] On 21 February 2008, this Office was contacted by officials from Eastern School District ("ESD") who notified us that a break and enter had occurred at Eastern School District offices, and four laptop computers had been stolen. One of the stolen computers contained a database of student information, including student names, MCP numbers, addresses, grade levels, phone numbers and names of parents/guardians. It is this laptop that is at issue in this Report. In all, 28,000 students were affected. ESD asked this Office to carry out an investigation with respect to whether there had been a privacy breach.

[2] I would like to note that during the course of this investigation, ESD was an active and willing participant and responded to all of our questions and requests for information in a most timely and cooperative manner.

[3] ESD informed us that the data contained on the hard drive of the laptop at issue was being used by one manager within ESD, whose role was, in part, to collect student information from schools and place students on the map to facilitate bussing and zoning. The personal information had been copied from the main server to the laptop to enable this manager to work from his home after hours and to enable him to immediately answer queries with respect to the planning process when meetings were held off-site and/or after hours. The manager was also giving presentations in District schools to illustrate the importance of collecting complete information about students so that bussing and zoning issues could be resolved. However, it is important to note that personal information was not disclosed during these presentations. The data on the laptop was used to generate a graphical illustration, that is, schools were shown on maps with dots representing students, and this illustration was used to show how bus routes and school zoning issues are worked on the basis of student demographical information.

II DISCUSSION

Response to Breach and Security Measures in Place

[4] Part IV of the *Access to Information and Protection of Privacy Act* (the "*ATIPPA*") was proclaimed into force on 16 January 2008. This part of the *ATIPPA* deals primarily with the protection, collection, use and disclosure of personal information. Shortly after the privacy provisions were proclaimed, this province's Department of Justice ATIPP Office published a document entitled "Key Steps When Responding to a Privacy Breach" (the "Key Steps"). ESD contacted the ATIPP Office shortly after the breach, and it is clear that ESD correctly identified and applied the appropriate framework, as outlined in the Key Steps, within which to approach this situation.

[5] According to the Key Steps, the first step in the process is to contain the breach. Unfortunately, this was not fully possible in this case, as the laptops were stolen and to date, have not been recovered. This means that while it is difficult to determine with certainty if the information was even accessed by the thieves, the breach is technically still occurring. However, network accounts of those identified as the owners of the stolen laptops were disabled. This would prevent access to the district's internal network (where all student, staff administrative information is kept) by a would-be hacker. The information on the hard drives of the laptops was protected by the Windows XP operating system, with strong passwords enforced. Strong passwords are characterized by a combination of upper and lower case letters, numbers and punctuation characters. They are at least 8 alphanumeric characters long, are not a word in any language and are not based on personal information.

[6] In addition to disabling network accounts of affected users, ESD also completed a thorough scan of all server systems located at ESD headquarters, including scans with McAfee Antivirus Enterprise and Windows Defender. No malware, spyware or virus activity was detected. A review of the Cisco PIX 515E Firewall configuration was also completed to ensure no changes were made to the configuration that would compromise access security. No such changes were detected.

[7] The second step in responding to a privacy breach is to evaluate the risks. This is necessary in order to determine what other steps are immediately necessary and what precautions should be taken in order to minimize, as much as possible, the chance of another breach occurring. Evaluation of the risks includes a consideration of several factors, including the type of personal information involved, the cause and extent of the breach, the individuals affected by the breach and foreseeable harm resulting from the breach.

[8] In this case, the breach affected a significant number of people, approximately 28,000 children and their parents, guardians or emergency contacts. The information on three of the laptops consisted of "applications-only" software, with user files stored on the network. Information on the fourth laptop consisted of student names, addresses, phone numbers, dates of birth, MCP numbers, schools, grades, parents'/guardians' name and contact information and bussing data. Fortunately, Social Insurance Numbers were not on the laptop. Nevertheless, while each separate piece of information that was contained on the laptop may not be considered highly sensitive (when compared to personal health information, for example), taken all together, this information could be used for illicit purposes in the hands of the wrong person, and the extent of the breach was quite far reaching, considering the number of people involved.

[9] The third step in responding to a privacy breach is notification and this is directly related to analysis of the above noted factors. Evaluation of the risks assists in determining whether notification is necessary, and if so, how it should be done and what information it should contain. The more sensitive the information, the more important the notification and the manner in which it is done becomes. Once people are aware of the breach and what information was potentially or actually exposed, they, along with the public body, can take appropriate steps to mitigate any potential risks associated with the information being disclosed.

[10] Again, in this case, it is impossible to determine whether the information on the laptop has been accessed. The police do not know who stole the laptops or for what purpose. It is impossible to determine that the laptops were stolen for their street value and not for the information contained on them, and therefore it is somewhat difficult to assess, with certainty, some of the above noted factors. **For the purposes of this Report, I will assume that the**

information has been accessed. Given the sensitivity of the information and the potential for harm if this information was misused, I believe that ESD acted appropriately in notifying the parents or guardians of all the children whose personal information was contained on the laptop. It is also my opinion that ESD chose effective means (news release, web notification and letters sent home with all children from affected schools) to do so.

[11] The fourth step in responding to a privacy breach is prevention. The cause of the breach must be thoroughly investigated, and safeguards and policies must be created or updated and implemented to minimize, as much as possible, the risk of another breach occurring. In this case, the cause of the breach was a break and entry resulting in the theft of the laptops, one of which contained personal information.

[12] At the time of the breach, the information on the laptops was protected by passwords only. No encryption software was installed on any of the laptops. The office space from which the laptops were stolen has one main entrance and three exit-only fire escape doors. Elevator access and entry to the reception area of ESD offices was unrestricted during business hours, while after hours, the main entrance to the office space (i.e. the reception area) from the hallway was locked, with a "card swipe" system for entry. As well, after hours, personnel entering the building signed in with building security and elevators were only operable by an access card (which is different from the swipe card for office entry) or by security guards. Two of the fire escape doors were also monitored.

[13] Subsequent to the theft, officials at ESD began to examine ways in which to improve security. ESD met with the landlord with a view to enhancing building security and issued a directive requiring that individual offices be locked nightly. In the actual ESD offices, a new office access/security system, which had been tendered and started in Fall 2007, was reassessed and upgraded in response to the breach. The new system maintains the after hours "card swipe" access to the reception area and also provides for security cards, complete with photo identification, to be issued to ESD personnel. Security cards must now be worn by all employees, and temporary "guest" or "visitor" cards will also be required for guests and consultants who

need to work inside ESD offices. After guests have finished their business at ESD, these temporary cards are collected by ESD personnel.

[14] Additionally, the new system provides for monitoring of the third fire escape door and also provides for enhanced access control within the ESD office space. In order to access the actual offices (located beyond the reception area, through a locked door), employees must swipe their security card. Guest access to the office area beyond reception is provided by front desk personnel, once people have been appropriately identified.

[15] In addition to upgrading the office security system, notebook locking mechanisms were ordered for all laptops deployed in the ESD headquarters and regional offices. This hardware consists of a thick carbon tempered steel cable, a T-bar locking mechanism and a combination lock, and includes an anchor-point to be secured to all users' desks which will provide a fixed point to secure the steel cable. When affixed to the anchor point or another immovable object, physical removal of the laptop is very difficult. This security measure has now been implemented. It is also my understanding that additional cable locks, for use in individual schools, have been ordered and received and will be implemented in some schools in September.

[16] Immediately following the breach, ESD issued a directive mandating that no personal information be stored on laptop computers. However, where circumstances require an exception to this rule, authorization from the ESD Finance and Administration Office must be obtained. In order to safeguard personal information that must be stored on laptops, ESD officials decided to implement the use of power-on passwords, BIOS passwords, hard disk drive passwords and encryption software (a process whereby data is encoded to render it unreadable except by authorized users). The power-on password is required as soon as the system is powered on, before access to general operating system functions is permitted and even before the BIOS **(**basic input/output system that determines what a computer can do without accessing programs from a disk) can be accessed, thus prohibiting potential tampering with BIOS settings. The BIOS password prevents the computer from fully booting unless the correct password is provided and the hard disk drive password prevents the drive from retrieving data unless the correct password is provided. Encryption software was used to encrypt a separate drive where personal

information must be stored, once proper authorization has been sought and obtained in accordance with the above noted directive. This directive remains in place even though all laptops in the ESD/regional offices now have these additional security features installed.

[17] With respect to the passwords noted above, I am informed by ESD that each user formulated their own passwords (i.e. none of the passwords are manufacturer standard issued) and the only people who know the passwords are the individual user and the IT manager for EDS, who stores them in an encrypted file.

[18] ESD has also now implemented a Department of Education directive requiring that all data on portable storage devices (i.e. flash drives, memory sticks, CD's) be encrypted. In order to ensure encryption is completed and secure, ESD has purchased encrypted flash drives, rather than rely on "add-on" encryption software to encrypt regular flash drives. Use of encrypted flash drives and implementation of the encrypted drive on laptop computers in ESD schools is planned for September.

[19] ESD has also contacted the laptop manufacturers and have planned internet seminars, conference calls and meetings so that these vendors can share recommended best practices and procedures that are available with their proprietary hardware and software offerings. ESD has also had an external security audit of their computer system completed and are now in the process of enhancing network security as recommended by the audit.

[20] In addition to the above noted Department of Education directive, ESD has also implemented several other directives, including "Network Administrators in Schools" (which governs the number of network administrators in schools), "Securing Servers in Schools" (which governs the physical security of servers in schools) and "WINSchool Passwords and Administration" (which covers the use of strong passwords within the WINSchool system).

[21] Several other policies and directives are currently in draft form and are under active review, including "After Hours Access – 6th Floor – Atlantic Place" (which will require presentation of a picture ID to building security in order to gain access to the sixth floor after hours), "Office

Guest – Contractor Access Policy" (which will govern guest access to ESD offices during business hours), "Acceptable Laptop Use Policy" (which will govern general security practices and care that all users of laptops must adhere to), "ESD Password Policy" (which will govern passwords to ensure integrity, strength and secrecy of passwords is not compromised), "Computer Disposal Policy," "Consultant Non-Disclosure Agreement" and "ESD Procedure for Wiping Computer Data." ESD is reviewing these policies in conjunction with the other four school districts, Memorial University, College of the North Atlantic and the Department of Education. These entities have joined to form the Provincial Education Protection of Privacy Committee and are working to develop uniform standards of privacy protection for the education sector. The drafts of these policies that this Office has seen are encouraging.

[22] In an effort to educate staff about access to information and protection of privacy, ESD also organized and presented an access to information and protection of privacy information and training session to all school administrators within the district and prepared a handbook of "Frequently Asked Questions" regarding the *ATIPPA* as a reference tool for educators.

Sufficiency of New Security Measures - Requirements under the *ATIPPA*

[23] As noted, the privacy provisions of the *ATIPPA* came into force on 16 January 2008. Under these provisions, a public body, such as ESD, has a statutory obligation to protect personal information from unauthorized use or disclosure and may only collect personal information for limited purposes. For the present purpose, the relevant sections are sections 32, 36, 38 and 39.

[24] Section 32 states as follows:

> *32. No personal information may be collected by or for a public body unless*
>
> *(a) the collection of that information is expressly authorized by or under an Act;*
>
> *(b) that information is collected for the purposes of law enforcement; or*
>
> *(c) that information relates directly to and is necessary for an operating program or activity of the public body.*

[25] Undoubtedly, a public body such as ESD must collect certain personal information for record keeping purposes, safety and legal purposes, as well as for planning and policy purposes. Names, addresses, and phone numbers (both home and work) of parents/guardians, emergency contact information and perhaps even some medical information (i.e. allergies) must all be collected by schools. However, I do question the collection of MCP numbers by ESD.

[26] When asked about this practice, ESD responded that the Department of Education standardized MCP numbers as their key identifier many years ago. The numbers are used by the Department for the Provincial Annual General Return (a count of all students in kindergarten to grade 12 in the province), public exam marks entry, special services database and many other uses. Therefore, ESD must collect and maintain this information in its internal student information system. As this identifier was already in use by the Department, ESD adopted it as their key identifier as well.

[27] Neither the *Schools Act, 1997* nor the *Medical Care Insurance Act, 1999* contains any explicit authority for the collection of MCP numbers by schools, school districts or the Department of Education. When asked to explain how MCP numbers are "necessary for an operating program or activity" of the Department, ESD replied that it was not in a position to explain this, and stated that due to the number of years that MCP numbers had been used, there may not be anyone at the Department level who could provide such explanation either. ESD noted that unique student identifiers could be created, however due to the Department's use of MCP numbers, ESD would still have to collect MCP numbers.

[28] Despite the fact the MCP numbers have been used as student identifiers for many years, we are now operating within a new set of rules. As previously stated, the privacy provision of the *ATIPPA* just came into force in January 2008, and some departmental policy changes may be necessary in order to comply with these provisions. Unless the Department can demonstrate that it is meeting the requirements imposed by Section 32 with respect to the collection of MCP numbers, it should revisit the policy of collecting and using MCP numbers as student identifiers.

From a privacy standpoint, a more desirable practice would be to adopt unique and random identifiers for students which each of the province's school districts could then also adopt.

[29] Regarding the use of personal information, section 38 states as follows:

> *38. (1) A public body may use personal information only*
>
> *(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose as described in section 40 ;*
>
> *(b) where the individual the information is about has identified the information and has consented to the use, in the manner set by the minister responsible for this Act; or*
>
> *(c) for a purpose for which that information may be disclosed to that public body under sections 39 to 42 .*
>
> *(2) The use 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 used.*

[30] I am, for the most part, satisfied that the information collected is used in accordance with section 38. The only aspect of use that I question is whether the use of the personal information in the course of the presentations discussed above would comply with section 38. However, I will leave that determination for another time, as the breach was not related to the use of the information at these presentations and the presentations themselves did not disclose personal information. Personal information was used to generate dots (which represented actual students) on a map and no identifying information was disclosed. Nevertheless, I would like to point out that usage of real data is not necessary in these presentations. Masked or scrambled data could be used for this purpose and, in fact, this is exactly what ESD has been doing since the breach.

[31] With respect to disclosure of personal information, section 39 states:

> *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.*

It is clear that in this case, the disclosure was not in accordance with this section.

[32] Turning now to section 36, which is the main focus of this Report, it 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.*

[33] This section requires public bodies to make "reasonable security arrangements." At paragraph 13 of Report P-2008-001, I quoted with approval British Columbia's Information and

Privacy Commissioner (Report F06-01) with respect to this standard of reasonableness, and it bears repeating here:

> *[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.*

[34] To determine whether ESD took "reasonable security measures" to protect personal information, I will consider the following factors:

1. The foreseeability of the privacy breach
2. The seriousness of potential harm (discussed above)
3. The cost of preventative measures
4. Relevant standards of practice

1. Foreseeability of the Privacy Breach

[35] As briefly discussed above, prior to the break-in, ESD considered its office space to be physically secure. It has still not been determined how the thieves gained access to ESD offices. After hours, persons entering the building in which the office is housed had to sign in with building security, elevators are only operable by security guards or an access card and access to the ESD office area is locked, with a card swipe system for entry (different than the elevator access card). The laptops were only minimally protected with passwords, however ESD has

advised that the laptop was housed, for the majority of the time, at the ESD offices. It was removed from the office only when the authorized user gave presentations at district schools and when he took it home to do work after hours.

[36] To point out the obvious, the very nature of a laptop is that it is readily mobile. While the laptop may have been normally kept in an office with multiple physical security features, the fact remains that it is portable. A laptop can be easily hidden, and carried out of an office unnoticed. Thefts of laptops have been and continue to be well publicized (see Alberta Information and Privacy Commissioner's Investigation Report P2006-IR-005 for a brief review of some recent well publicized cases). The Office of the Privacy Commissioner of Canada recently released its Annual Report to Parliament 2007 wherein it states that half of the data breaches reported to it related to electronically stored data, often customer information stored on laptop computers that had been stolen.

[37] Given the portability of laptop computers, the street value of the computer itself as well as the personal information it contains, the increase in cases of laptop theft and the fact that these computers and the information contained therein were minimally protected, I believe the breach was reasonably foreseeable, despite the perceived security of the building. Although the theft was not, in this case, due to employee inattention or carelessness, the comments of Alberta's Commissioner in Report P2006-IR-005 are still relevant:

> *Absolute supervision of a laptop is not possible, and is a fact thieves count on. Leaving the security of laptops entirely to employees is not reasonable given that laptops can be stolen from their homes or even taken from them forcefully…. Human nature and circumstances beyond the control of an employee must be accounted for when organizations consider personal information safeguards. Other lines of defense are critical.*

2. Seriousness of Potential Harm

[38] The seriousness of potential harm was discussed in paragraph eight and need not be repeated here.

3. Preventative Measures and Cost

[39] The first and most obvious way to protect personal information vis-à-vis laptop computers is simply not to store personal information on laptops. As noted above, laptops are prime targets for thieves and absolute supervision of laptops is just not possible. However, I understand that this simple solution is not an option for many public bodies. Employees must travel, and/or work after hours and the majority of files and information they require in order to carry out this work are stored electronically. Therefore, laptops and the storage of personal information on laptops are a necessity for some employees. As such, where storage of personal information on laptops cannot be avoided, increased vigilance and effective security measures are necessary. These security measures encompass administrative, physical and technological means.

[40] Limiting access to personal information is one reasonable way in which to protect personal information. Essentially, this administrative measure entails a "need to know" policy. Personal information should only be provided to those who reasonably need to know it. This is accomplished in two ways – by allowing access to personal information only to certain individuals (who reasonably require access in order to carry out their employment duties) and by allowing access to only the specific information required to perform employment duties. Minimizing the number of people who have access to personal information as well as minimizing the amount of personal information a particular individual has access to is a basic method by which to protect personal information, as less access means less opportunity for unauthorized use or disclosure.

[41] At the time of the breach, ESD had such a policy in place. This policy, entitled "Acceptable Use of ICT Policy" explicitly covers data storage and use and prohibits anyone from attempting to access information that they should not have access to, and prohibits those with administrative rights from accessing data except in certain specific circumstances. This policy also recommends a maximum of 2-3 network administrators for large schools. In this case, the data on the laptop was used by an employee in the course of his duties, and some of his work was completed after hours, making use of a laptop necessary.

[42] Physical security is also important. Use of cable locking mechanisms or docking stations to secure laptops to desks reduces the ease with which they can be picked up and taken. Secure office space and locked individual offices are also reasonable and inexpensive measures that can be undertaken to prevent theft of computers and the information they contain.

[43] Technological security also has a great role to play in protecting personal information. Operating system passwords are easily circumvented, even with strong passwords enforced. Free or inexpensive software and instructions are available on the internet to "crack," reveal or simply bypass such passwords, thus allowing a thief to access all data in locally-stored files. As noted, password protection was the sole form of security installed on the stolen laptops.

[44] A more secure method of protecting data is through encryption. As briefly noted earlier, encryption is a process whereby data is encoded to render it unreadable except by authorized users. In order to encrypt and decrypt data, a key or an algorithm must be used. The more complex the algorithm, the harder the encryption is to break; for example, 128 bit encryption is stronger than 56 bit encryption. There are various types of encryption; I choose not to comment upon specific types of encryption, as what is necessary and practical may vary depending on the circumstances and the sensitivity of information involved.

[45] Strong encryption technology is widely available through numerous vendors at reasonable prices. This Office was able to find, with minimal searching, good encryption software available for just over $100 per perpetual license. Encryption tools and software are also available free of charge on the internet and several Microsoft Windows systems have various encryption capabilities pre-installed. This technology is therefore widely available and the cost is not prohibitive.

[46] Other available technology includes remote tracking of computers and remote data deletion. To give a brief overview of one such remote tracking program, a software agent is installed on the laptop and each day the computer is connected to the internet, it reports its location, user, hardware and software information to a confidential monitoring centre. After a laptop has been reported stolen, this program is automatically set up to call the monitoring centre every 15

minutes. The data delete function is similar in that after a laptop has been stolen, the owner can set up a "data delete" request so that the next time the computer calls the monitoring centre, the data stored on the computer will be deleted. After this has been done, data is no longer recoverable, even by the proper owner. This particular software is available on a per machine subscription basis and costs about $100 for a three year subscription.

[47] In Investigation Report P2006-IR-005, Alberta's Information and Privacy Commissioner also discusses similar technology:

> *[51] Tracking systems or "phone home" software for mobile devices that can trace the physical location of a laptop (even if the hard disk is reformatted and the operating system reloaded) are also available for roughly $130 per device for three years of service. Some tracking systems are also offered with encryption, and the combination may be purchased in single quantities for approximately $80 annually. These combinations create an encrypted partition on the hard drive. A thief can obtain access to the system and will appear to have wide use of it. However, he or she will not see any of the files in the encrypted partition because the system will not display that part of its directory. Meanwhile, "IP tracking" or even GPS location information signals are being sent to a "home" server each time the stolen laptop is connected to the internet.*
>
> *[52] In order to retain control over data on a missing laptop, some organizations are examining a technology called a "kill switch". Similar to tracking services, a stolen laptop periodically connects with an Internet server. If the server notes that the laptop is flagged as stolen, it initiates a series of actions to prevent unauthorized access or sends "self-destruct" instructions. The "self destruct" command can also be set to proceed after certain events such as repeated failed password or authentication attempts, removal from pre-determined locations, travel further than preset distances, or connection via foreign or unauthorized networks. Single-user pricing for this service is less than $200 annually per laptop.*

[48] As noted by Alberta's Commissioner in the above noted Investigation Report, "While the cost for different strengths, types and management strategies for data safeguards may vary, they are arguably less than an organization's cost of recovering from a data breach."

4. Relevant Standards of Practice

[49] The ease with which laptops can be inconspicuously removed from any location, secure or not, requires a heightened degree of security and vigilance with respect to protection of personal or sensitive information. Information technology professionals advocate the use of multiple layers of security when trying to protect personal information. Essentially, this entails the use of several different types of safeguards, including administrative (i.e. policies, programs and directives), physical (i.e. cable-locking mechanisms, locked cabinets, locked rooms, etc) and technical (i.e. encryption, remote tracking and remote delete). Multiple layers increase the "hoops" thieves have to jump through in order to access the information. Arguably, the longer it takes, and the more troublesome it is for thieves to succeed, the less likely they are to continue their efforts.

[50] A search of the internet returned many sites with tips from IT professionals on how to prevent laptop theft and protect documents. Some of these tips include:

- Use computer-locking cables/docking station
- Asset tag or engrave the laptop
- Register the laptop with the manufacturer
- Encrypt sensitive data
- Use tracking software
- Enable a strong BIOS password
- Use personal firewalls
- Disable the infra-red port (otherwise others may be able to browse files at a distance without even touching the computer)
- Disable the guest account
- Rename the Administrator account/Create a dummy Administrator account
- Carry the laptop in a nondescript case
- Never, ever leave the laptop unattended anywhere, anytime or any place

As can be seen, these tips include both physical and technological means for protecting laptops and the information they contain from theft. Obviously, if an organization were to employ any of these measures, their use should be supported and formalized by policies and directives mandating the use of such measures.

[51] Information and Privacy Commissioners across Canada are recognizing the need for enhanced protection of personal information stored on mobile devices. The Privacy Commissioner of Canada stated the following in her Annual Report to Parliament:

> *We hope the growing awareness about the need to alert our Office and affected individuals about privacy breaches will soon translate into more effective security measures. We continue to urge individuals and organizations to take basic data security precautions such as:*
>
> - *Limit the amount of personal information collected, used and carried on electronic devices;*
> - *Never leave a laptop unattended where it could be stolen;*
> - *Use technologies which enhance security and privacy such as data encryption and anonymizing services;*
> - *Use hard-to-crack passwords;*
> - *Avoid automatic login features which save user names and passwords; and*
> - *Ensure that personal information is completely overwritten – not just deleted – from a hard drive before discarding or selling a computer*
>
> *By following these steps, organizations can significantly reduce the risk that the personal information they hold will be compromised.*

[52] In Investigation Report P2006-IR-005, Alberta's Commissioner concluded that three layers of security are necessary to protect personal information; physical, administrative and technical. With respect to technical measures, the Commissioner stated as follows :

> *Information technology media has been full of articles about the importance of encryption on laptops. Recent incidents of corporate laptop thefts have solidified its relevance. This technology is already available on standard operating systems and can be easily obtained or purchased. Although decrypting an encrypted file is*

> *not impossible, it requires a high and rare degree of skill and time, making it a reasonable safeguard in the context of PIPA. Of course, organizations may consider any number or combination of the security measures discussed other than encryption.*

[53] More recently, on 7 May 2008, British Columbia's Information and Privacy Commissioner issued Investigation Report F08-02 following an investigation into the loss of tapes containing personal health information. The tapes were lost while in transit between New Brunswick and British Columbia via courier. The Commissioner found that given the nature of the information, the failure to use encryption and the ease with which a tracking policy could have been implemented, the Ministry of Health had failed to take reasonable measures to protect personal information against unauthorized disclosure or use.

[54] In Order HO-004, Ontario's Information and Privacy Commissioner ordered that the Hospital for Sick Kids implement a policy, applicable to both desktop and portable devices (laptops, PDA's, etc.) mandating that personal health information not stored on secured servers must either be de-identified (scrambled or masked such that the individual to whom the information pertains cannot be identified) or encrypted. This Order was the result of an investigation into a data breach that occurred when a laptop was stolen from a minivan.

[55] Included in Order HO-004 was a "Commissioner's Message," which I would like to set out here in its entirety, as it too discusses the multi-layered approach to information protection, with an emphasis on technological measures. While this message specifically pertains to personal health information, the standard of reasonableness is also applicable in that case, and therefore, I believe the message contained therein is applicable to all personal information which must be protected on a reasonableness basis:

> *Mobile computing devices, including laptop computers, flash drives and PDAs are widely deployed in the health care sector in Ontario. Such devices can provide enhanced capabilities for health care providers and enhanced services for patients. But such benefits may also come at a price. The risk of theft or loss of mobile computing devices is known to be high. While laptop computers are often stolen for the value of these devices, in some cases, thieves are becoming increasingly interested in the personal information that they contain. There is no way of distinguishing one kind of theft from another. Personal information stored*

on stolen devices can be used for purposes such as fraud and identity theft – problems that have reached epidemic proportions throughout North America. And with the movement of organized crime into this area, the problem takes on a greater and more sinister complexion.

In the present incident, while the stolen laptop happened to contain PHI that was being used for research purposes, it could have contained PHI that was being used for any purpose, either inside or outside of the health care facility. Therefore, all health information custodians using mobile computing devices to store PHI can learn from this unfortunate, but predictable, incident.

Health information custodians are required under the Act to take steps that are reasonable in the circumstances to ensure the PHI is protected against theft, loss and unauthorized use or disclosure. Accordingly, it is my view that it is no longer reasonable to store PHI on mobile computing devices, unless steps are taken to ensure that any PHI stored on such devices is protected against unauthorized access, in the event that the device is lost or stolen. A multi-layered approach is needed to guard against unauthorized access.

As a first line of defence against unauthorized access, custodians should avoid storing identifiable PHI on mobile computing devices. However, where PHI must be stored on such devices, only the minimal amount of information necessary should be stored, and for the minimal amount of time necessary to complete the work. In addition, whenever possible, PHI should be de-identified or coded, in a manner such that the identities of the individuals whose PHI is stored on the device could not be readily ascertained if the information were accessed by unauthorized persons. If the information is coded, the code that is needed to unlock the identities of individuals should be stored separately on a more secure computing device, such as a central server in a health care facility.

Another layer of defence against unauthorized access is the use of password protection. In many circumstances, this is not sufficient, as in this case. Strong passwords consist of at least eight characters and combine letters, numbers and symbols in what appear to be random strings. However, because passwords may be guessed, written down, stolen, shared, hacked or cracked with software that is readily available, they are often the weakest link in the security chain. Consequently, it is my view that password protection alone can no longer be considered to provide adequate protection against unauthorized access to PHI stored on mobile computing devices.

Where identifiable PHI is stored on vulnerable devices, such as laptop computers or flash drives, my position is that the information must be encrypted. At a minimum, files or folders containing PHI should be encrypted. It is essential to use up-to-date encryption techniques to ensure that personal information is appropriately secured. If the chosen encryption technology or software requires a password as a key, then strong passwords, as described above, should be used.

The encryption of files and folders should not rely on a user's login password due to the above-noted vulnerabilities associated with such passwords. Similarly, users should know not to use login passwords as passwords to decrypt files and folders. Custodians should look for encryption software packages that have built-in mechanisms to enforce the use of strong encryption keys.

In addition to the encryption of individual files or folders using strong encryption keys, it is also possible to encrypt an entire hard disk within a laptop computer. Full disk encryption is a type of software or hardware that can be used to protect all the data on a hard disk, including the operating system, resident data, temporary files, and deleted files. Other disk encryption software can be used to protect everything on a hard disk, except the operating system.

The importance of information security has been carefully considered by the state of California, which has taken the lead with many privacy and data security issues. In 2002, California enacted breach notification legislation that requires all organizations to notify California residents when their unencrypted, computerized personal information is, or is reasonably believed to have been, acquired by an unauthorized person. Given that no company wants to tell customers that its systems were, for example, "hacked" and sensitive data was accessed, the potential effect of this law's mandatory notification highlights the advantages to encrypting information as a means of avoiding embarrassing privacy breach incidents.

Consequently, to the extent that personal health information on a mobile computing device has been encrypted to protect it from unauthorized access, I would not consider the theft or loss of that device to be a loss or theft of PHI. The Act requires custodians to notify an individual at the first reasonable opportunity if PHI is stolen, lost or accessed by unauthorized persons. If the case can be made that the PHI was not stolen, lost or accessed by unauthorized persons as a result of the loss or theft of a mobile computing device because the data were encrypted (and encrypted data does not relate to identifiable individuals), the custodian would not be required to notify individuals under the Act.

I would also like to advise health information custodians that there is an emerging focus on data security and information breaches, not only in the United States, but also in Europe. Recently in the United Kingdom, its financial services regulator levied a substantial fine against a building society, following the theft of an employee's laptop that contained personal information relating to approximately 11 million customers. In addition to being fined, the organization was heavily criticized for failing to adequately address the risk that customer data might be lost or stolen and for having inadequate security procedures. This case illustrates the importance of the security of personal information, and the lessons learned may easily be applied in the health sector.

> *Therefore, I strongly urge all health information custodians to regularly review their privacy and security policies and procedures relating to the storage of PHI on mobile computing devices to ensure that they are effective in minimizing the significant risk to privacy posed by the loss or theft of such devices. All custodians should invest in proactive measures to protect PHI stored on mobile computing devices. In the event that a mobile computer device is lost or stolen, this would save custodians time and money by allowing them to avoid the notification requirements of the Act, and prevent the potentially irreparable damage to a custodian's reputation resulting from the loss or theft of PHI. More importantly, it would protect individuals from the undue stress of knowing that their PHI had been lost or stolen.*
>
> *There is no excuse for unauthorized access to personal health information due to the theft or loss of a mobile computing device – any PHI contained therein must be encrypted.*
>
> [Emphasis added]

[56] Canada's *Personal Information Protection and Electronic Documents Act* codifies, in Principle 4.7.3 of Schedule 1, a multi-layered approach to information security:

> *The methods of protection should include*
>
> *(*a*) physical measures, for example, locked filing cabinets and restricted access to offices;*
>
> *(*b*) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and*
>
> *(*c*) technological measures, for example, the use of passwords and encryption.*

[57] The federal government has implemented a multi-layered approach in its "Operational Security Standard: Management of Information Technology Security (MITS)." This is a standard pursuant to the *Government Security Policy and the Policy on the Management of Government Information* and it states, in part, as follows:

16.4.3 Authorization and Access Control

Departments must restrict IT and information access to individuals who have been screened and authorized; have been identified and authenticated; and have a "need to know."

Departments must keep access to the minimum required for individuals to perform their duties (i.e., the least-privilege principle), and ensure that they are regularly updated to accurately reflect the current responsibilities of the individual.

Departments must withdraw access privileges from individuals (including students, contractors, or others with short-term access) who leave the organization, and revise access privileges when individuals move to jobs that don't require the same level of access.

16.4.4 Cryptography

When properly used, cryptography is an effective means of ensuring confidentiality, integrity, authentication and non-repudiation. Departments must ensure effective key management, including the protection and recovery of cryptographic keys.

Departments must use encryption or other safeguards endorsed or approved by the Communications Security Establishment (CSE) to protect the electronic communication of classified and Protected C information. Departments should encrypt Protected A and B information, when supported by a Threat and Risk Assessment. However, departments must encrypt protected B information before transmitting it across the Internet or a wireless network.…...

16.4.7 Mobile Computing and Teleworking

Off-site use of departmental IT assets can introduce additional information security risks. Departments that allow personnel to access departmental information and IT assets, networks and systems from outside their government offices must establish procedures for such use.

To protect the remote computer, the information it contains, and the communications link, departments should use an effective combination of physical protection measures, access controls, encryption, malicious code protection (e.g. virus scanners), backups, security configuration settings (e.g. operating system controls), identification and authentication safeguards, and network security controls (e.g. a PC firewall).

> *Departments must ensure that personnel working off-site are made aware of their security responsibilities, including the sensitivity and criticality of the information and IT assets they access.*

[58] The Office of the Chief Information Officer, Government of Newfoundland and Labrador, also recommends that one "always encrypt files or use an encrypted USB flash drive when e-mailing, storing or transferring personal and or confidential files."

[59] Clearly, a multi-layered approach to safeguarding personal information is the standard. With respect to technological measures, encryption appears to be the accepted and trusted industry standard, and this is not unique to Canada.

[60] Encryption of personal information stored on mobile devices is also the standard recommended practice in the United States and the United Kingdom. In June of 2006, the Executive Office of the President (United States), Office of Management and Budget issued a memorandum directing all US agencies and departments to "encrypt all data on mobile computers/devices which carry agency data unless that data is determined to be non-sensitive…" As noted in Alberta Investigation Report P2006-IR-005, and in Ontario Order HO-004, in several US states, (California, in particular) only laptops enabled with data encryption are exempt from notification requirements. Presumably, data protected by encryption is secure to the extent that even if it is lost, a breach cannot be said to have occurred, therefore, there are negligible risks associated with the loss and notification is not necessary.

[61] On their website, the United Kingdom's Information Commissioner's Office states as follows with respect to their approach to encryption:

> *The ICO recommends that portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.*

[62] As a multi-layered approach to information security is the current industry standard, I am also of the opinion that this approach is necessary for compliance with section 36 of the *ATIPPA*. At the time of the breach, ESD was not using this approach. Some useful physical safeguards were in place, but administrative and technological safeguards were obviously lacking. While directives and policies alone would not have prevented this breach, they are nonetheless an important feature in safeguarding personal information. In another case, policies and directives may be the difference between a breach occurring or not. In this situation, however, appropriate technological measures may have prevented the breach. Use of network passwords alone to protect personal information does not constitute a "reasonable security measure" as mandated by section 36 of the *ATIPPA*. This lack of adequate technological safeguards led to unauthorized disclosure of personal information, contrary to section 39.

[63] However, since the breach ESD has gone a long way towards implementing a multi-layered approach and has significantly enhanced safeguards. Regarding the administrative layer of security, ESD has a policy (in place prior to the breach) limiting the number of people who have access to personal information stored on the network, and reasons for which they can access it. Immediately following the breach, ESD implemented a directive prohibiting the storage of personal information on laptops. Where circumstances dictate otherwise, authorization to do so must be granted, and then it will be stored on the encrypted drive of a laptop that is protected by three layers of password security. This directive remains in place. Further, ESD is also in the process of developing additional policies to safeguard personal information. In addition to these policy initiatives, ESD conducted *ATIPPA* information sessions with school administrators, and prepared a handbook for easy reference for educators. I am satisfied that these initiatives are in keeping with the requirements of section 36 but I would caution ESD to ensure all privacy policies, once finalized, are distributed to and read by all employees. Periodic auditing to ensure these policies are being followed is also a recommended practice.

[64] With respect to physical security, I am satisfied that the safeguards currently in place are also reasonable. Building and office security has been enhanced, and cable locking mechanisms are now in use at the ESD offices. In fact, prior to the theft, I believe it can be said that the security system in place was a "reasonable security arrangement." As mentioned, the standard

imposed by the *ATIPPA* is that of reasonableness, not perfection. Thieves broke into a secure space and stole these laptops. No security system is infallible and this case was certainly not an instance of employee carelessness or negligence. The comments above to that effect are included solely for their educational value to other public bodies whose employees use and transport mobile devices containing personal information.

[65] Having laptop computers protected solely by a network password is clearly insufficient as a technological safeguard, given the current standards of practice for protection of personal information, this does not meet the reasonableness standard imposed by the *ATIPPA*. As noted above, encryption technology is readily available and simple to implement, and is necessary in order to protect personal information that must be stored on laptops. ESD has now installed encryption software on all district/regional laptops, and will also soon be installing encryption software in some schools. In addition, there are three layers of password security now in place on District laptops. I am satisfied that these technological safeguards are also adequate with respect to the standard imposed by section 36.

V CONCLUSION

[66] I would like to conclude by quoting Alberta's Information and Privacy Commissioner in Investigation Report P2006-IR-005:

> *[37] The risk of corporate laptops being stolen is well known and foreseeable. In most cases this occurs inadvertently: individuals naturally forget, become distracted or are outsmarted, victimized, swayed by convenience or may even apply their own acceptable risk threshold to a situation despite laptop handling policies. Although policies are necessary, without technical security measures that go beyond employee compliance, the likelihood that an unauthorized user could gain access to data stored on mobile devices is relatively high. Previous privacy findings as well as federal legislation recommend encryption as one reasonable measure of protection to guard against well known risks.*
>
> ……
>
> *[61] An organization need not implement each and every available security measure. However, it is well established that simple log-on passwords and employee watchfulness is insufficient. Organizations should apply multiple layers*

> *and measures that give personal information adequate protection**.** I have identified encryption as one possible technical safeguard because it is readily available and simple to use.*
>
> [Emphasis added]

[67] ESD breached sections 36 (with respect to the protection of personal information) and 39 (regarding disclosure of personal information) of the *ATIPPA* by not having reasonable safeguards in place to protect personal information which then resulted in unauthorized disclosure of personal information. However, ESD appears to have taken this breach very seriously, and since then, has taken multiple actions to protect personal information in accordance with section 36 in order to reduce the likelihood of such a breach occurring in the future. ESD's approach to protection is now consistent with relevant standards of practice across the country, and once policy development is complete, it is my opinion that ESD will have successfully implemented a multi-layered approach to information security vis-à-vis laptop computers. Further, the measures ESD has chosen to implement are consistent with recognized industry standards. As such, I believe it can now be said that reasonable measures to safeguard personal information are now in place.

[68] While I am not in a position to determine if collection and use of MCP numbers are directly related to or necessary for an operating program or activity of ESD or the Department, if this cannot be established, there is a breach of section 32 of the *ATIPPA*. However, even if the requirements of section 32 can be met with respect to the collection of MCP numbers, I suggest that collection and use of MCP numbers by ESD or the Department is not a "best practice". Otherwise, there was no breach of sections 32 or 38 of the *ATIPPA*. Collection and use of all other information mentioned herein is in keeping with these sections.

VI RECOMMENDATIONS

[69] ESD has, on its own initiative, taken adequate steps to enhance safeguards with a view to protecting personal information that must be stored on laptops. The approach taken by ESD

encompasses several layers of protection and I am satisfied that this meets the "reasonableness" requirement set out in section 36. Therefore, I have only one recommendation as follows:

- that ESD, in partnership with the Department, generate and assign random and unique identifiers to students to replace the use of MCP numbers. These identifiers can then be used in the same way as MCP numbers are currently used, but without the risk of disclosing personal information should the identifiers be disclosed.

[70] ESD is requested to please respond to this recommendation within 15 days of receiving this Report.

[71] Dated at St. John's, in the Province of Newfoundland and Labrador, this 23rd day of July, 2008.

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