Nova Scotia Personal Information International Disclosure Protection Act

2008 Annual Report

NS Information Access and Privacy Office

Message from the Minister of Justice

I am pleased to provide the third Annual Report regarding public body decisions to permit foreign access and storage of personal information, as authorized under the *Personal Information International Disclosure Protection Act* (PIIDPA). PIIDPA was created to enhance provincial privacy protection activities, and at the same time respond to Nova Scotian concerns about the vulnerability of public sector and municipal personal information holdings to foreign access, storage and disclosure. The Act prohibits public sector entities, municipalities and their service providers from allowing foreign storage, disclosure or access to personal information, except to meet the "necessary requirements" of a public sector or municipal operations.

Under PIIDPA subsection 5(3), Nova Scotia public sector entities are required to report the decision and description of any foreign access and storage of personal information occurring from January 1, 2008 to December 31, 2008 to the Minster of Justice. This report is based on the public sector reports received by the Department of Justice.

This report contains a summary of the 44 public sector and municipal entities who reported access or storage of personal information outside Canada, as subject to provisions within PIIDPA. This report describes the decisions made, the conditions or restrictions placed, and reasons explained by the public bodies to allow storage or access of personal information in its custody or under its control outside Canada after the PIIDPA was introduced. Note: 13 entities reported that there was no access or storage outside of Canada for the 2008 calendar year.

_____

Honourable Ross Landry

Minister of Justice and Attorney General

SUMMARY OF SUBMITTED *PIIDPA* REPORTS

A: Description of the decision of the public body to allow storage or access of personal information in its custody or under its control outside Canada.

B: Conditions or restrictions that the head of the public body has placed on such storage or access of personal information outside Canada.

C: Reasons resulting in the head of the public body allowing storage or access of personal information outside Canada to meet the necessary requirements of the public body's operation.

Table 1: Summary of January 1, 2008 – December 31, 2008 Foreign Access and Storage by Government Departments[1]

Department	A (Description)	B (Conditions)	C (Reasons)
Agriculture	The Laboratory Information Management System (LIMS) Project Team (inclusive of Information Technology representation) evaluated software and the selection was an upgrade with the current service provider. This company is housed in the United States and has been our service provider for nine (9) years.	Historically, there was no restriction. The programmer gained access to LIMS via pcAnywhere software. The LIMS system contains clients sample submission and analysis information.	The access was only granted trouble shooting system errors and only at the request of the client (Laboratory Services). Only three systems meet the criteria for our LIM system requirements. The three systems were evaluated with the resultant decision to go with our current service provider. In summary: a)Manitoba LIMS was only able to match 6 features that both CLIMS and Automatic Technologies Inc. (ATI) were able to provide. b)VLIMS had all the same 17 features as ATI, with the additional 7 features as follows: 1.Windows 2005 program 2.Server connection Microsoft SQL Service 2005 TCP/IP 3. Use of a word processor for typing

[1] NS Environment reported that no personal information was accessed or retained outside of Canada.

Department	A (Description)	B (Conditions)	C (Reasons)
			in diagnosis 4.Tracking of logins and changes to reports 5.Auto fax, e-mail in process – pdf format 6.Can flag reportable diseases 7.Entering of results in one field (not moving from one field to another) 8.Ability to produce labels and use a bar coding system 9.Can be customized (no charge for up to one (1) year) 10.Accounting package (generates invoices and receipts) 11.Ability to do Turn around times for each Lab section 12. Inventory program available 13.In house administrative functions 14.Crystal reports program for

Department	A (Description)	B (Conditions)	C (Reasons)
			statistics 15.Feature to flag client duplication 16.Has the ability to add Feeds, Waters, etc., at a later date 17.Is able to link with the Public Health Agency of Canada (PHAC) database for their and Canadian Food Inspection Agency (CFIA) data needs under Canadian Animal Health Surveillance Network (CAHSN) Unique to system purchased: 1.Transfer of data from existing system (1999-2007), so no data is lost 2. Maintenance agreement with server support 3.Program support using pcAnywhere – 24 hour support 4.Expressed knowledge of Accreditation 5.Equipment interfacing – 3 pieces of

Department	A (Description)	B (Conditions)	C (Reasons)
			equipment included in the cost 6.Additional training sessions are available using pcAnywhere, at no cost 7.Lowest bid The critical deciding factor to utilize a US firm was the addition of items 1-7, in particular, no data lost and the lowest bid. Laboratory Services deals in surveillance programs for animal health with the Federal Government and is required to maintain a data base of clients and diagnosis. This data would not have been readily transferable into any system other than the Windows version of the current system.

Department	A (Description)	B (Conditions)	C (Reasons)
Economic Development [(NSED), now called Economic and Rural Development]	NSED was presenting sponsor of the Power of Green Conference, October 20, 2008. The Conference registration process was completed on a secure website. The website and registration database was developed by Rampage Technology, as the service provider. The personal information (name and contact information) used for registration purposes was collected and stored on a dedicated server owned by Rampage and hosted by maximum ASP, Louisville, Kentucky, USA (subcontractor).	Because Rampage had a dedicated (not a virtual) server, Maximum ASP did not have any control over the server unless Rampage specifically gave permission to make a physical change which Rampage could not execute. The data was only used for the Power of Green Conference registration website purposes and was permanently deleted from the server when the administrator deleted it.	The decision to permit disclosure of personal information of Conference registrants outside Canada enabled NSED to discharge its responsibilities as conference presenting sponsor by providing seamless and efficient online registering for Conference participants.
Education (DOE)	a. The Department utilizes Oklahoma Scoring Services (OSS) software for the purpose of storing and processing information, in support of the General Educational Development (GED) program. The GED is an internationally recognized assessment tool of high school equivalency. The GED credential is accepted by employers	a. The Department has signed a contract with OSS, which stipulates that all information will be kept private and confidential, and will not be released to any third party unless authorized by the Department in writing. The contract also states that only personnel authorized by the department will be provided	a. The department completed an evaluation of options for the delivery of the NS GED program in November 2001. It was determined that two, suitable for Canadian requirements, GEDTS certified vendors were located in the USA. The application service provider (ASP) model included storage of the data at a vendor location in the USA. At the present time, there is no

Department	A (Description)	B (Conditions)	C (Reasons)
	across NS and Canada, and serves as an important function for labour mobility. The GED is comprised of five tests that measure the skills corresponding to those of recent high school graduates. There are approximately 1500 tests conducted each year in NS. The department scans the test sheets locally and sends data to OSS over a encrypted Sockets Layer (SSL) connection, or in some cases by traceable courier. The information is stored in a database at OSS located in Norman, Oklahoma for processing and as a record for future reference. Continued storage is required for data retrieval and combining score results for students re-writing tests that were not passed successfully. Should the department terminate services with OSS the data will be returned/transferred to the department or another service provider, and removed from the OSS database.	access to store and retrieve NS information.	option of a software solution with data storage in Canada. The other option available in 2001 was to custom develop a system to manage the GED program, and then apply for certification as a testing facility with GEDTS. This option was not chosen due to cost and time constraints to conform to GEDTS program changes in 2002. This would have resulted in an interruption in client service to allow time to design the system and obtain certification from the GEDTS. The department's decision to contract with OSS was based on their extensive experience in GED test scoring, maturity of the software solution, security methods used for transmission of information, and good reputation across educational jurisdictions. In addition, OSS came highly recommended by GEDTS.

Department	A (Description)	B (Conditions)	C (Reasons)
	The test scoring is completed remotely by OSS and the test results and certificates are transmitted to the department in PDF files for printing locally. The transmission is over a SSL connection or a Virtual Private Network (VPN). The test results and certificates are also available for viewing by authorized DOE staff on the OSS web site, using the same security methods, a user ID and password. In addition, the information is transferred by OSS to the General Educational Development Testing Services (GEDTS) international database, which contains information used for statistical reporting of GED achievements by jurisdiction. This includes gender, age, country, province, number of participants, number passed, number failed and other information. GEDTS is located in Washington, DC, the international database is		

Department	A (Description)	B (Conditions)	C (Reasons)
	housed by Marsys in Miami, Florida, and the backup database is housed by Marsys in San Mateo, California. The international database was established to support the GED program and it is mandatory that jurisdictions agree to send data to GEDTS as part of the GED licensing agreement. b. A number of staff from the Department of Education traveled outside Canada and had ability to access personal information carried on email or stored in GroupWise via remote access to GroupWise email system, using devices such as BlackBerry's and laptops. c. Nova Scotia Provincial Library (NSPL) maintains an integrated library system (ILS) on a cost-recovery basis for a consortium consisting of 63 branch libraries in eight regional library systems, and four government department libraries. The ILS provides a library catalogue, a purchasing module, and a circulation module	b. Remote access to GroupWise is protected by username/password authentication, and is delivered over an SSL encrypted link. c. NSPL has implemented reasonable security measures to protect personal and other information in the ILS. The ILS software is maintained on a secure server in Brunswick Place. The contract with the company stipulates that NSPL staff must be contacted when the company requires access to the ILS server. NSPL enables	b. When staff are traveling for business reasons they are expected to monitor their email and voice mail where possible in order to fulfill their responsibilities. c. The decision was made to continue with SirsiDynix because there is no Canadian alternative. There are four major ILS vendors in the world who offer systems with the functionality required by libraries in the NSPL consortium, none of which are Canadian. When NSPL chose Sirsi in 2003, the company was a Canadian

Department	A (Description)	B (Conditions)	C (Reasons)
	(check-in/check-out, and client information). Without an ILS, the libraries could not operate; this service has been identified in the Department of Education's Business Continuity Plan as "Essential" (Level 3). The ILS contains personal information about identifiable individuals (library clients in Nova Scotia), including name, address, telephone number, an identification number, and library materials currently on loan to the individual. The client's personal information is voluntarily given when she or he registers for a library card. The inventory of materials a client has on loan from a library is available only until materials are returned and subsequently cleared from the client's account. The ILS is owned by an American company, SirsiDynix, and access to personal client information from outside Canada is possible with SirsiDynix. There is no Canadian	SirsiDynix to access the server for specific upgrade activities at predetermined time periods, at the end of which SirsiDynix staff are logged out by NSPL staff. NSPL staff monitor and audit to ensure the access is reasonable and appropriate. SirsiDynix has no operational requirements to access personal information about clients. Therefore, the risk of access to personal information about Nova Scotians by SirsiDynix is low, but it is technological possible.	corporation. In 2005, Sirsi was purchased by Dynix, an American company. The company serves customers worldwide from its base in the United States.

Department	A (Description)	B (Conditions)	C (Reasons)
	vendor which supplies a similar product.		
Finance	a. It is necessary that remote access to provincial SAP systems be performed by SAP Support Staff via secure network connections to provide routine and emergency support maintenance. Following a management approval process, access occurred several times throughout the reporting period as required to correct or troubleshoot various problems within the SAP systems. Access was only from SAP's own internal support network and carried out by SAP staff resident in SAP locations, such as the United States, Germany, and India. This remote access very rarely involves access of personal information, but in cases where this access does involve potential access to personal information for the purpose of resolving a specific	a. When SAP Support Staff have reason to access any of the Province's SAP systems as part of a problem remediation, all production system transaction access is approved by the Corporate Information Services (CIS) Division management and all access activity is recorded in an audit log so that some verification can be done of whether personal information is accessed. In addition, this access occurs over secure network connections that prevent other parties from gaining access to the SAP systems. When access is granted to SAP Support Staff, specific controls on the time and duration of that access are maintained.	a. Access by SAP Support Staff is required from time to time in order to assist the CIS Division with remediation of technical problems with the SAP systems managed by the Division. This access is controlled by the Province and there is no transaction to SAP systems permitted without the knowledge and approval of Division management. SAP provides their support services from international locations, in multiple time zones. There is currently no alternative method of support access for the SAP systems that would preclude access from outside Canada. These remote access services are required to meet the mandate of the CIS Division in the performance of services to various public sector organizations who use SAP.

Department	A (Description)	B (Conditions)	C (Reasons)
	support problem, records and audit logs of that access are maintained. b. It was necessary for Government Accounting staff, who are authorized, and who were out of the country, to access the provincial SAP systems (Financials) via a secure remote network connection in order to provide routine and emergency support.	b. Access to the SAP system occurred over a secure network connection that prevents other parties from gaining access to the SAP systems. TS web access control software is used in the Provincial government to ensure the protection of personal information while being accessed remotely. Access is restricted and controlled by the Province and no transactions to SAP systems are permitted without the knowledge and approval of Division management.	b. There is a limited number of staff in Government Accounting who are authorized to perform routine and emergency support for the SAP (Financials) system. Remote access services are required to meet the mandate of the Government Accounting Division in the performance of services to numerous departments.
Health.	a. Between January 1, 2008 and December 31, 2008, fifty-two (52) staff of the Department of Health traveled outside Canada on business and had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise System.	a. The DOH *Transmission of Confidential E-mail and Fax Guideline* (2004) prohibits the inclusion of personal email sent outside the GroupWise system unless the e-mail is encrypted and password protected. The Guideline also recommends limiting the inclusion of personal information contained in e-mail	a. When staff is traveling for business reasons (e.g. meetings, conferences) they are expected to monitor their e-mail and voice mail where possible. Therefore, it is necessary for them to check e-mail remotely where possible in order to fulfill their responsibilities.

Department	A (Description)	B (Conditions)	C (Reasons)
		within the GroupWise system. Therefore, the amount of personal email held or sent by e-mail, and therefore available for access while staff were outside the country, should be limited.	
	b. FirstWatch Solutions is a provider of data monitoring and biosurveillance software and related services to organizations and agencies in the fields of public health and public safety. Emergency Health Services (EHS) through its contractor, Emergency Medical Care Inc. (EMC) utilizes a hosting system, called FirstWatch that stores a copy of the Computer Aided Dispatch (CAD) on a server located in San Diego, California. The CAD system captures information related to all calls for service including emergency 911 calls and transfer services. FirstWatch, as a hosting service allows data from several sources to be consolidated into one location	b. The Agreement with FirstWatch includes provisions requiring compliance with all applicable Canadian Federal, Provincial and Municipal statutes, and regulations, including but not limited to the *Freedom of Information and Protections of Privacy Act*, *Personal Information International Disclosure Protection Act*, and the *Personal Information Protection and Electronic Documents Act*. The agreement includes explicit provisions related to requirements for maintaining the confidentiality of all confidential/private information, personal information and "Protected Health Information"	b. First Watch, as a hosting service allows data from several sources to be consolidated into one location and formatted easily for review and interpretation. It allows for faster decision making with regards to injury and disease surveillance, monitoring and allows access to the information being collected in real time, which would not be possible without the application. There is no company in Canada that would provide this level of service.

Department	A (Description)	B (Conditions)	C (Reasons)
	and formatted easily for review and interpretation. It allows for faster decision making with regards to injury and disease surveillance monitoring and allows EHS to better monitor system performance and allows access to the information being collected in real time, which would not be possible without the application. There is no company in Canada that would provide this level of service.	(PHI), including: - limitations on the use and disclosure personal information; - making reasonable security requirements against all risks, including but not limited to tampering, theft, sabotage, unauthorized access, collection, use, disclosure and disposal of PHI; - reporting any unauthorized disclosure of PHI; - requirements for handling requests for access to personal information; - notification to EHS of any attempted or actual tampering, theft, sabotage, unauthorized access, collection, use, disclosure and disposal; - notification to EHS of any request, demand, subpoena, warrant, order issued or used by	

Department	A (Description)	B (Conditions)	C (Reasons)
		a foreign authority or court.	
Health Promotion and Protection	There was no storage of personal information in the custody or control of the Department of Health Promotion and Protection outside of Canada from January 1, 2008 to December 31, 2008 Between January 1, 2008 and December 31, 2008 twelve (12) staff members from the Department of Health Promotion and Protection traveled outside Canada on business and had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise System.	The Department of Health Promotion and Protection *Transmission of Confidential Information by E-mail and Fax Guideline (2004)* prohibits the inclusion of personal information contained in e-mail, unless the e-mail is encrypted and password protected. The Guideline also recommends limiting the inclusion of personal information contained in e-mail within the GroupWise system. Therefore, the amount of personal information held or sent by e-mail, and therefore available for access while staff was outside the country, should be limited.	When staff are traveling for business reasons (e.g. meetings, conferences) they are expected to monitor their e-mail and voice mail where possible in order to fulfill their responsibilities.
Intergovern-mental Affairs	In 2006 the Department of Intergovernmental Affairs entered into a service contract with Iron Mountain Canada Corporation (a Canadian subsidiary of Iron Mountain Incorporated) for the storage of paper records, which are not accessed regularly, but are not	Iron Mountain is to contact Intergovernmental Affairs upon the receipt of a subpoena or similar order unless such notice is prohibited by law. Confidential information shall be held in confidence by Iron Mountain and shall be used only	This decision was made to address the issue that Intergovernmental Affairs has limited space while at the same time business activities create records that remain relevant for long periods of time. Iron Mountain specifically was chosen because at the time no Canadian owned competitor in Nova Scotia could

Department	A (Description)	B (Conditions)	C (Reasons)
	ready for storage at the Government Records Center. The offsite storage/retrieval/shredding vendor is a subsidiary of a US based company. The information is not transferred outside of Canada.	in the manner contemplated by the agreement. Iron Mountain will use the same degree of care to safeguard this information as it utilizes to safeguard its own confidential information.	be found. Furthermore they are considered to be their industry lead. Intergovernmental Affairs is currently revising its records management policies with the intent to terminate the relationship with Iron Mountain and rely solely on the Government Records Centre.
Justice	a. For 2008 there were 9 employees who traveled outside Canada and many have accessed personal information through email during that time. b. JEMTEC Inc. was chosen to provide Electronic Supervision of Offenders monitoring and services to Nova Scotia and was awarded the contract in December 2007 for Electronic Supervision of Offenders. All personal information is stored in secure databases located in secure Monitoring Centres owned/operated by JEMTEC and approved	a. Remote access to GroupWise is protected by username/password authentication, and is delivered over an SSL-encrypted link via the secure Blackberry GroupWise server. b. The restrictions included: 1. JEMTEC's project manager and the Provincial Electronic Supervision Coordinator shall be the only persons authorized to establish user accounts (logins and passwords) for the host monitoring system. 2. JEMTEC's Project Manager	a. When staff is traveling they are expected to monitor their email for operational purposes. b. This access was necessary to ensure optimal service and to maintain automated monitoring systems that communicated system issues, such as hardware failures, software abnormalities, or other operating environment issues that may arise. JEMTEC/Omnilink personnel require access to the operating system and software in order to complete regular system maintenance functions required

Department	A (Description)	B (Conditions)	C (Reasons)
	subcontractors, which include BI Inc., and Omnilink Inc., located in Toronto, Canada, Boulder Colorado, U.S., and Alpharetta, Georgia, U.S., respectively.	shall immediately notify DOJ of all relevant details of any unauthorized access. JEMTEC's Project Manager shall document the reason the access occurred, the person/agency who accessed the information, and the time, date, specific data compromised and duration of the access. JEMTEC's Project Manager shall verify what steps have been taken to prevent further unauthorized access. 3. The system contains a journal function original to the software to allow system and program management user access to an audit trail of all changes made to an individual's file or its data content (e.g., offender address, contact information, scheduling of calls, termination of offenders from the program), as well as who made the change, when it was made and what the change consisted of. This provides senior administrators with a tracking tool for quality control	to ensure mission critical operation of the system. This contract was terminated on December 10, 2007, and the contractors indicated in the report are receiving no further information.

Department	A (Description)	B (Conditions)	C (Reasons)
		and data security purposes. Access to the systems is via a standard internet browser with 128 bit SSL encryption, with predefined timeouts to lock out users after periods of inactivity after they have logged in, for security purposes.	
	c. JEMTEC Inc. was awarded the contract for Voice Verification of Offenders. All personal information is stored in secure data bases located in secure Monitoring Centres owned/operated by JEMTEC (including its subcontracted monitoring services), BI and Biometric Securities – located in Toronto, Canada, Boulder, Colorado, US and Decatur, Georgia, respectively.	c.1. JEMTEC's project manager and the Provincial Electronic Supervision Coordinator shall be the only persons authorized to establish user accounts (logins and passwords) for the host monitoring system. 2. Only JEMTEC Inc. and DOJ personnel designated by DOJ shall have "permanent" user access to the host monitoring system. JEMTEC's Project Manager shall document the reasons the access occurred, the person/agency, who accessed the information, and the time, date, specific data compromised and duration of the access. JEMTEC's Project Manager	c. This access is necessary to ensure optimal service and to maintain automated monitoring systems that communicate system issues, such as hardware failures, software abnormalities, or other operating environment issues that may arise. JEMTEC Inc. and its subcontractors require access to the operating system and software in order to complete regular system maintenance functions required to ensure mission critical operation of the system.

Department	A (Description)	B (Conditions)	C (Reasons)
		shall verify what steps have been taken to prevent further unauthorized access. 3. The VoiceID system contains a journal function original to the software to allow system and program management users access to an audit trail of all changes made to an individual's file or its data contents (e.g., offender address, contact information, scheduling of calls, termination of offenders from the program), as well as who made the change, when it was made, and what the change consisted of. This provides senior administrators with a tracking tool for quality control and data security purposes. Access to the VoiceID system is via a standard internet browser with 128 bit SSL encryption, with predefined timeouts to lock out users after periods of inactivity after they have logged in, for security purposes.	
	d. In July 2004, the Department of Justice entered into a service		

Department	A (Description)	B (Conditions)	C (Reasons)
	contract with Iron Mountain Canada Corporation to provide document destruction and government record storage.	d. In 2005, the Department of Justice reviewed the physical and procedural security and access environment at Iron Mountain Canada Corporation in Hammonds Plains.	d. The Department of Justice entered into this contract as there was insufficient storage available at the Records Centre.
Natural Resources	There was no storage of personal information in the custody or control of the Department of Natural Resources outside of Canada from January 1, 2008 to December 31, 2008. a. Five staff members traveled outside Canada on business and had the ability to access personal information via remote e-mail, Blackberry, personal computer or by any other means. b. Two staff members traveled outside Canada on pleasure and had ability to access personal information carried on e-mail or stored in GroupWise via remote access to GroupWise e-mail system. c. Off site record storage contracted	a. Remote access to GroupWise is protected by username/password authentication, and is delivered over an SSL-encrypted link. b. Remote access to GroupWise is protected by username/password authentication, and is delivered over an SSL-encrypted link. c. Iron Mountain is to safeguard	a. When staff are traveling for business reasons they are expected to monitor their e-mail and voice mail where possible in order to fulfill their responsibilities. b.When staff is traveling for pleasure they are sometimes required to maintain contact with operations. c. Offsite storage of backup

Department	A (Description)	B (Conditions)	C (Reasons)
	with Iron Mountain Canada (subsidiary of the American Company).	and maintain protected storage of the Department's records. Iron Mountain Canada Corporation confirms that personal information is maintained and disclosed in accordance with our contractual arrangement in compliance with all applicable legislation.	media/microfilm is required as part of the Disaster Recovery Program. The offsite storage is required to ensure recovery of vital records can be recovered should an incident occur.
Office of the Premier	In 2006, the Department of Intergovernmental Affairs entered in a service contract with Iron Mountain Canada Corporation (a Canadian subsidiary of Iron Mountain Incorporated) for the storage of paper records which is not accessed regularly, but is not ready for storage at the Government Records Centre. The offsite storage/retrieval/shredding vendor is a subsidiary of a US based company. The information is not transferred outside of Canada.	The service contract with Iron Mountain states: - Iron Mountain is to contract Intergovernmental Affairs upon the receipt of a subpoena or similar order unless such notice is prohibited by law. - Confidential information shall be held in confidence by Iron Mountain and shall be used only in the manner contemplated by government. - Iron Mountain shall use the same degree of care to safeguard the Confidential Information of Intergovernmental Affairs as it	This decision was made to address the issue that Intergovernmental Affairs has limited space while at the same time business activities create records that remain relevant for long periods of time. Iron Mountain specifically was chosen, because at the time no Canadian owned competitor in Nova Scotia could be found. Furthermore, they are considered to be their industry lead.

Department	A (Description)	B (Conditions)	C (Reasons)
		utilizes to safeguard its own confidential information.	
Public Prosecution Service	There was no storage of personal information outside Canada by the Public Prosecution Service. There was access to personal information using wireless data devices, including BlackBerry's and laptops, on a daily basis while staff were visiting outside of Canada.	The conditions placed on such access involved the use of encryption and password protection.	Such access was granted in order to permit those staff to discharge some of their responsibilities while absent from their offices.
Service Nova Scotia and Municipal Relations (SNSMR)	a. The Inter-provincial Record Exchange (IRE) system allows Canadian motor vehicle jurisdictions to securely query other jurisdiction's driver and vehicle records. The Canadian Council of Motor Transport Administrators (CCMTA) disseminates the IRE information, administers the system and operates the secure network. There is a partnership arrangement with the American Association of Motor Vehicle Administrators (AAMVA) to extend the IRE system to the US.	a. CCMTA acts as the clearing house for all queries so that jurisdictions do not have direct read access to another jurisdiction's system. Queries are forwarded to/from member jurisdictions only (CCMTA & AAMVA). Queries are pre-formatted and specific as to what information is displayed. CCMTA has contracts with each of its member jurisdictions that conform to the jurisdictions' privacy legislation concerning disclosure and consent.	a. Promotion of road safety and law enforcement so that a driver's license or vehicle permit may not be fraudulently transferred from one jurisdiction to another. b. Access by Digimarc is an operational

Department	A (Description)	B (Conditions)	C (Reasons)
	b. Digimarc, of Fort Wayne, Indiana, was awarded the contract to provide Photo Licence/Photo ID equipment, software integration and support services for the Registry of Motor Vehicles in 1999. The current contract expires in 2008 and will be replaced with a new contract under the joint Atlantic Canada Photo License Project. One component of the system, the Photo License Oracle server that stores client photos, digitized signatures, personal information, and Driver Master Number is located at the Provincial Data Centre in Halifax. In 2006, two Digimarc support technicians were provided remote access via VPN to provide tier II/III support. Routine maintenance and support for this system is provided by a local Digimarc field technician, with the Fort Wayne technicians acting as back-up, or managing escalated problems the local technician isn't able to resolve. c. Nine SNSMR staff members traveled outside Canada during the	b. Access from the Fort Wayne location is restricted via VPN username/password to these two support technicians and on the Oracle server by a privileged account username/password. Access will be in response to escalated support calls only. c. Remote access to GroupWise is protected by Username/Password	requirement in response to Photo Licence/ Photo ID outages that affect the delivery of customer service. c. To maintain contact with operations.

Department	A (Description)	B (Conditions)	C (Reasons)
	reporting period and accessed GroupWise e-mail from a laptop or Blackberry™ while away. d. An American company, Tyler/CLT, was given controlled access to Assessment for the purpose of converting and transferring that data from the Assessment legacy system to the new iasWorld system. Tyler/CLT continues to have controlled access to the system, which houses Assessment data for the purpose of servicing and maintaining the system. For security reasons all data remained in Canada, and remote access by Tyler/CLT was tightly controlled.	authentication, and is delivered over an SSL-encrypted link. d. Contractor access is only allowed through a restricted and audited VPN account. Contractors can only access a terminal server, which has been configured for the purposes of doing the data conversion. The terminal server is configured to not allow data transfers to other computers, i.e., the contractor cannot mail or copy the file to themselves or another network. Contractor activity is reviewed and monitored via the audit logs.	d. The iasWorld system was the only Computer Aided Mass Appraisal (CAMA) system that would meet all the Assessment Divisions requirements. Competing Canadian systems were examined during the RFP process, but did not meet requirements. The American company Tyler/CLT serviced the Assessment legacy system and produced the core CAMA component of the new iasWorld system. Therefore they were the only organization with the expertise to convert the data from the old system to the new, and to service iasWorld on an ongoing basis.
Tourism, Culture and Heritage	a. Nova Scotia Archives and Records Management: Decision to allow primary service provider (Unisys Canada Inc.) for Internet resource NOVA SCOTIA HISTORICAL VITAL STATISTICS ONLINE (NSHVSO)	a. No disclosure to, or retention of credit card personal information by service subprovider outside Canada except as required to carry out and verify online commercial transactions with NSHCSO.	a. Commercial component of NSHVSO online service depends on client's ability to prepay for copies online via credit card transaction conducted in real time. Due to the global character of today's financial services industry, it is extremely

Department	A (Description)	B (Conditions)	C (Reasons)
	operated by NS Tourism, Culture and Heritage (Archives and Records Management Division) to outsource to service subprovider (Skipjack, Cincinnati, Ohio, USA) part of the transaction processing, and storage during processing, of credit card information collected from service clients during online interactive commercial activity.		unlikely that online credit card transactions can be completed and verified without the personal information collected during transaction processing being stored, accessed from or disclosed outside Canada.
	b. Tourism: The Department has contracted Cloutier Direct Inc. (CDI) of Scarborough, Maine to mail Nova Scotia tourism information to people who have requested Nova Scotia information from the U.S. and internationally. Requests are received though their customer contact system, call centre, which is based in Halifax; through the Novascotia.com web site and through regular mail requests. On a daily basis CDI downloads from their contact centre, U.S. and International requests and sends out the requested information. The Department contracted Bristol	b. Names and addresses may only be used to fulfill requests received by the Department. The Department owns the database. CDI may only use the names and addresses once unless approval is received from the Department. Only name and address fields were disclosed to Telematch. There were 16,000 records and the data was in their possession for 31 days. Telematch used one (1) day for processing the data and then maintained the data for 30 days on a secure processing server. After the 30 days the information was deleted.	b. The Department has contracted CDI to provide fulfillment services to ensure that the potential visitor to Nova Scotia receives their literature promptly in a cost effective way. The Department previously fulfilled U.S. and International requests from Canada and the delivery time was too long and too expensive for the service received. Require the use of this company as the information resides in the United States.

Department	A (Description)	B (Conditions)	C (Reasons)
	Omnifacts Research, St. John's, NL, to contact enquirers who requested Nova Scotia tourism information in 2008. This includes people who have requested Nova Scotia information from the eastern seaboard of the U.S. If neither an email address nor a telephone number were supplied, Bristol contracts Telematch in the U.S. to conduct a phone number look up based on the name and address provided to our customer contact centre or through the Novascotia.com web site, which are based in Halifax.		
Transportation and Infrastructure Renewal	a. Symphony Services, located in California, was awarded a contract in 2006 by the PNS to supply and support an Expense Management System (EMS) which is used by the PNS Telecom Services Group to re-bill, on a monthly basis, all telecommunication costs to PNS users. A report was filed by the Minister of Transportation and Public Works pursuant to subsection 5(3) of the Personal	a. Symphony Services will not have the ability to remove or copy files. Once the conversion is complete, access will be disabled and only re-enabled during scheduled support services work. Symphony Services has read, understands and has signed off on *PIIDPA* obligations. Government employees on occasion may travel to	a. The EMS application was the best fit for the Telecom Service Group operational requirements. There were no cost-effective Canadian solutions available. Symphony Services has supplied the previous two telecom billing services, thus are familiar with the Provincial requirements. Their experience with migrating other clients to EMS lowers the Province's risks associated with migration of data. The EMS application

Department	A (Description)	B (Conditions)	C (Reasons)
	Information International disclosure Protection Act ("PIIDPA"), with respect to the award of the contract to Symphony Services in 2006. PNS subsequently renewed the contract is 2008 to permit Symphony Services to continue to provide support services for EMS. Symphony Services at times requires access to the EMS application and database in order to do scheduled support or troubleshooting work. This access is done through its office located in Dallas, Texas, and is executed remotely, using Microsoft's Terminal Services on a server located in the PNS data centre. Microsoft's Terminal Services provides three levels of authentication and is only made available by PNS to Symphony Services during scheduled times. When access is provided to Symphony Services it is monitored by PNS employees. b. Bell Aliant has entered into a	Symphony Services offices to inspect the security measures used to protect personal information. b. In the Long Distance Services	server will provide a stable, secure operating environment. The Department will be able to use the existing Oracle corporate licence agreement and will allow use of other current software that was not compatible with Tru Server. b. Due to the global nature of telecommunication operations and

Department	A (Description)	B (Conditions)	C (Reasons)
	Long Distance Services Master Agreement with the Province of Nova Scotia (PNS) to provide long distance services for PSN end users. In the course of providing the long distance service, Bell Aliant will have access to the PNS end users' personal information (names and telephone numbers). Bell Aliant may utilize customer service representatives located outside of Canada to provide troubleshooting and customer support activities to PNS end users. While providing these services to PNS end users, the customer service representatives located outside Canada may ask them to verify their personal name and telephone number.	Master Agreement, Bell Aliant acknowledges and confirms that all personal information (name and telephone number) provided to it by PNS is confidential and the information shall not, during the term of the agreement, or at any time thereafter, be disclosed to any third parties except as expressly permitted by the Agreement. Bell Aliant acknowledges and confirms in the Agreement that it is a "service provider" as defined in PIIDPA and that as a "service provider," it is bound by the obligations imposed on it by PIIDPA. Bell Aliant has agreed to comply with the obligations imposed on it as a service provider under PIIDPA. Bell Aliant's databases in which PNS end user personal information (name and telephone number) is stored are configured in a manner that allows it to control access to the databases, including the ability to restrict or	services, long distance providers capable of meeting PNS long distance requirements have facilities outside Canada that provide service and have the capacity to access and store PNS personal information (name and telephone number). The use of this personal information (name and telephone number) is only for the purpose of verifying ownership of the telephone number, to provide assistance in completing a long distance call, and to provide the fraudulent use of the long distance services by an unauthorized party.

Department	A (Description)	B (Conditions)	C (Reasons)
		deny access to those databases at any time. Bell Aliant has agreed to implement security measures to protect PNS personal information (name and telephone number) that it collects or uses in the performance of its obligations under the Agreement. It has also agreed to include in its standard contracting documentation with its service providers and suppliers outside of Canada who have access to PNS end user personal information (name and telephone number), the privacy and security obligations and restrictions that are applicable to Bell Aliant under the Long Distance Services Master Agreement. PNS can, upon giving ten (10) business days prior written notice to Bell Aliant, enter Bell Aliant premises during normal business hours for the purpose of conducting an audit to confirm	

Department	A (Description)	B (Conditions)	C (Reasons)
		the security measures it has taken.	
Communications NS	Under the Province of Nova Scotia privacy policy, Internet IP (Internet Protocol) addresses are considered personal information. For three Internet-related initiatives – Nova Scotia Come to Life website, Come to Life Pomegranate, and Building for Growth – we used a web statistical analysis service called Google Analytics that involved storing IP addresses on Google's servers in the United States.	This information is subject to the Google Privacy Policy. (The Google Privacy Policy outlines its responsibility to protect any personal information it collects against any unauthorized access, disclosure, or destruction. It further details that they will not share any personal information without prior consent unless it is to comply with applicable laws.)	Communications Nova Scotia is accountable in our business plan to report on the effectiveness of major Internet (and other) campaigns. Use of Google Analytics enabled us to collect and report on accurate statistics about how many visitors came to our websites, from where, and approximately how long they stayed. This information allows us to refine our marketing and advertising strategies ensuring that we provide best value to the government.
Film Nova Scotia	Approximately three staff members traveled outside Canada on business. These staff members had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise e-mail system.	N/A	When staff are traveling outside of Canada for business reasons, they are expected to monitor their e-mail in order to fulfill their job responsibilities.
Halifax-Dartmouth Bridge Commission	The Halifax-Dartmouth Bridge Commission implemented a new toll collection system in 2008. Part	Access to the locally maintained customer data must be achieved through a secured firewall	The Halifax-Dartmouth Bridge Commission maintains and operates two toll bridges which span the Halifax

Department	A (Description)	B (Conditions)	C (Reasons)
	of this system is an account management system for electronic toll collection, "MACPASS". The supplier of this system is headquartered in California and they provide development, implementation, support and maintenance services for this customer account application via remote VPN access to their systems which reside locally in the Commission's data centres.	appliance. All customer data must be maintained locally and within the Commission's isolated domain. The system uses Cisco firewalls to prevent undesired access to the system from outside terminals. The Commission has control of the firewall to grant access to any users who may work offsite. The servers employ SSH2; no clear-text user names or passwords are transmitted internally or externally. Secure copy and/or secure FTP are used for file uploads and downloads.	harbour. The most popular method utilized by the Commission to collect tolls is electronic toll collection, "MACPASS". This technology utilizes an account management system to maintain individual prepaid customer accounts. The nature of the Commission's toll collection application is unique and proprietary. An RFP process was used to procure the system and the successful proponent is based in the United States.
Utility and Review Board	Payroll details of Board members and staff were held by Ceridian Canada, a payroll service provider operating in Canada, but owned by a parent company resident in the United States.	Data was held as confidential records by the payroll service provider. Information was stored on servers located inside Canada.	Ceridian is the longstanding payroll provider for the Board. A Canadian company was located that processed payroll, but was unable to meet the boards needs.
Nova Scotia Business Inc.	a. Pursuant to s. 5(2) *PIIDPA* the head of Nova Scotia Business Inc. (NSBI) determined the	a. The business contact information is to be protected in accordance with the	a. NSBI requires a robust and secure CRM platform to store and manage information necessary for the conduct

Department	A (Description)	B (Conditions)	C (Reasons)
	storage/access outside Canada of business contact information in NSBI's custody/control, as part of customer relationship management (CRM) data services supplied under contract by salesforce.com inc (a Delaware, US corporation with its principle place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.	salesforce.com inc master agreement and privacy statement which recognize NSBI as owner of the stored data and provide strong privacy protection and security processes. The service is certified as a "Safe Harbor in confidence" under the EU Directive on Data Privacy and is certified "TRUSTe" privacy complaint.	of NSBI's relationships with its clients, prospective clients, partners and stakeholders. The Salesforce® data service was selected through independent evaluation and based on its superior standing in meeting predefined objective evaluation criteria (including service functionality, IT compatibility, data security, vendor experience and cost). The tangible risk of compromising these critical service requirements outweighs the remote risk of business contact information (given its more accessible public nature) being the target of a foreign demand for disclosure.
	b. Pursuant to s. 5(2) *PIIDPA* the head of NSBI determined the storage/access outside Canada of personal information (primarily business contact information) in NSBI's custody/control, as part of the investment attraction and trade development services supplied under contract by international in-market consultants (global) is to meet the necessary requirements of	b. The personal information (primarily business contact information) is to be protected in accordance with the service agreement including confidentiality provisions.	b. NSBI engages international in-market consultants as an essential and integral component of NSBI's trade development and investment attraction activities. The consultants are experts in the business environment within a business sector or geographic region of interest. International consultants operate from and travel outside Canada and must be able to store and access personal information (primarily

Department	A (Description)	B (Conditions)	C (Reasons)
	NSBI's operation. c. Pursuant to s. 5(2) *PIIDPA* the head of NSBI determined the storage/access outside Canada of personal information in NSBI's custody/control, stored in, or accessed using, a mobile electronic device by an NSBI director, officer, or employee for business continuity purposes during international travel is to meet the necessary requirements of NSBI's operation.	c. Personal information stored in or accessed using a mobile electronic device by an NSBI director, officer or employee during international travel is to have a reasonable and direct connection to the person's job duties and be protected by the director, officer or employee in accordance with the NSBI Code of Conduct and Oath of Office.	business contact information) outside Canada in order to facilitate business connections/transactions in performing their contracted services. c. For business continuity purposes, NSBI directors, officers, employees must be able to store and access using a mobile electronic device personal information that has a reasonable and direct connection to the person's job duties so the person can perform work responsibilities while traveling outside Canada.

Table 2: Summary of January 1, 2008 – December 31, 2008 Foreign Access and Storage by Health Authorities

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Annapolis Valley District Health Authority (AVDHA)	a. The software maintenance contract was awarded to Con-Test for a five-year period. b. It is estimated that 35 employees traveled outside of Canada for business and may have accessed personal information via laptop, Blackberry™ or PDA's.	a. N/A b. AVDHA has implemented encryption and passwords for laptops, Blackberry™ and PDA's.	a. N/A b. Current storage and access to personal information outside Canada is linked to existing programs, services and software utilized by AVDHA to ensure efficient operations.
Capital District Health Authority	Approximately 56 CDHA staff members traveled outside of Canada and may have (or had the ability to) access personal information via remote e-mail, Blackberry, personal computer or by any other means. Note: this does not reference physicians who have CDHA privileges.	CDHA general information and sharing policies apply in this situation. More specific guidelines related to access and storage of personal information outside of Canada is under development.	Current storage and access to personal information outside of Canada is linked to pre-existing programs and systems utilized by CDHA and are deemed necessary for management and operations.
Cape Breton District Health Authority (CBDHA)	a. Approximately 7 employees traveled outside of Canada and may have accessed personal information via remote e-mail or Blackberry™. b. CBDHA entered into 20 application	a. N/A	a. N/A b. Current storage and access to

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	maintenance contracts with the following vendors: Toshiba Canada and G.E. Diagnostic for diagnostic imaging; Fresenius Medical for renal dialysis; Varian Medical and Ventana for radiation therapy and pathology Benchmark XT, G.E. Diagnostics for EKG and Phillips Medical; G.E. Healthcare for lightspeed RT (CT scanner and workstation); Dictaphone Solutions for dictation system; Quality America for Q-Pulse Software; Siemens Canada Ltd. For mammography; Siemens Medical Solutions for mammography; 3M for HDM System and ANRS Modale; Beckman Coulter for LH75) Analyzer; Biomerieux for Vitek 2Xl and Bact Alert 240 Analyzers, Ortho Clinical Diagnostics for Vitros Analyzers and Oracle for Database		personal information outside Canada is linked to pre-existing programs and systems utilized by CBDHA and are deemed necessary for ongoing operations.
Colchester East Hants (CEHHA)	Approximately three staff members traveled outside of Canada and may have accessed personal information via remote e-mail, Blackberry™ or Treo™ No contracts were renewed or signed	Guidelines will be developed relating to access/storage of personal information outside of Canada.	Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized by CEHHA and are deemed necessary in the ongoing operations of these systems

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	during this reporting period.		and programs.
Cumberland Health Authority (CHA)	VPN access to Dictaphone System, Florida, for remote vendor application support. VPN access to Saturn OR system from US for remote vendor application support. Encrypted (SSL) staff access to CHA web mail system from US locations. Storage of information on whole disk encrypted CHA owned laptops.	Access to information stored on CHA networks and servers is only permitted through encrypted VPN connections. All external e-mail access is encrypted through SSL, VPN or the Blackberry™ service. The CHA has adopted a standard for encrypting all information on laptops and media that is released outside the CHA, including removable media such as encrypted USB storage devices and CD/DVD's. Established a process whereby all business changes that may affect the release, use or access to private information are reviewed regularly by the Privacy and Information Management	Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized in the CHA and are deemed necessary in the ongoing operations of these systems and programs.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		committees. Privacy Impact Analysis must be completed on all new systems.	
Guysborough Antigonish Strait Health Authority (GASHA)	There have been less than five decision made to allow the storage or access of personal information outside Canada. This is related to staff travel outside of Canada who are cognizant of PIIDPA and GASHA's policies and procedures on privacy.	Access to information from outside Canada is restricted to this legislation and permitted only for the purposes of conducting GASHA business. Vendors must agree to follow PIIDPA legislation. Staff are required to follow GASHA's Privacy Policies and Procedures.	New systems that manage or contain personal identifiable information must undergo a Privacy Impact Analyses. Limitations are placed on vendors who may require access for maintenance procedures as 24/7 access to personal identifiable information is never permitted.
Pictou County Health Authority (PCHA)	Access and storage from outside Canada is linked to pre-existing programs and/or systems utilized at PCHA which continue to be required to be used for the necessity in ongoing operation of these systems and programs (e.g., Meditech, Dictaphone, 3M). PCHA Senior Leaders may have accessed personal information while conducting business outside the country using remote e-mail and Blackberry.	Vendors are required to following PIIDPA legislation. Staff is required to follow PCHA's privacy policies.	Access and storage from outside Canada is linked to pre-existing programs and/or systems utilized at PCHA, which are required for ongoing operations of these systems and programs.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
South Shore Health Authority (SSHA)	SSHA entered into several contracts between January 1, 2008 to December 31, 2008 that may require access or storage of personal information outside Canada. (Please note that these contracts are under review by SSHA). The contracts are as follows: 3M Canada Inc., Agfa, BCE Emergis Inc., CareNET Services Inc., ECRI Institute, GE Medical Systems, IMP Solutions, Leica Microsystems Ltd., Muse Interational, Ormed Information Systems Ltd., Ortho Diagnostics, Siemens Medical Solutions Diagnostic, Somagen, Somagen Diagnostics Inc., and Summit Technologies Inc. South Shore Health as directed staff to refrain from the use of South Shore Health owned devices that contain personal information including Blackberry and cell phones while out of the country for pleasure or business. However, we recognize there may have been unauthorized access to information from outside the country	The following clause now appears in all Requests for Proposals and Tenders awarded by South Shore Health: "Vendor acknowledges that in the performance of any Contract awarded hereunder it may obtain information concerning individuals which information is subject to protection in accordance with applicable legislation and regulation including, without limiting the generality of the foregoing, the Personal Information International Disclosure Protection Act ("PIIDPA") Bill No. 19 and any other applicable Act or regulation. Vendor agrees to safeguard any such information in accordance with all such legislation/regulation and use same solely to comply with its obligations under the	Current storage and access to information from outside Canada is linked to pre-existing programs/software used within South Shore Health and is deemed necessary for continued operations. Specific criteria for allowing storage or access outside Canada will be developed as part of the District's policy for the protection of personal information from access outside Canada that is currently under development.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	using webmail or VPN. There were 7 out of country business trips approved during this period. South Shore Health is participating with other district health authorities and Department of Health in development of a policy for the protection of personal information from access outside Canada.	Awarded Contract.	
South West Nova District Health Authority (SWNHA)	Twelve staff members traveled outside of Canada and may have accessed personal information which included laptops, Blackberry, and web mail. There may or may not be others who traveled outside the country and used South West Health electronic equipment for operational reasons. For operational reasons there continues to be storage and controlled access of information in the area of Diagnostic Imaging, Dictaphone, etc. b. South West Health will be implementing a Financial, Human	An inclusion clause for contracts is now added to all Requests for Proposals, renewed or new co	Current storage and access of information is linked to the pre-existing programs/software utilized in the Health Care facility. The new SAP program best meets the needs of the health district and is being implemented in all health districts (this is the same program selected in other services such as municipalities, education); prior to implementation a privacy impact assessment has been completed.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	Resources, Materials Management and Payroll information system called "SAP". This is a provincial program. The following contracts are still under investigation re the ability to access personal information: Pitney Bowes; Siemens; G.E. Healthcare; Whidden Systems Ltd.; Cassa Business Equipment; Elsevier; Microtech Supply & Service Inc; Medhunters.com; Altima Technologies Inc; Eclipsys Corporation; East Coast Capital Inc; Britech; Ekahau; Guardian Edge Technologies; SharepointHQ; Xwave; IMP Solutions; Powerwright Services Inc; Info Tech; Somagen Diagnostics; Beckman Coulter; Inter Medico; Dominion Biological Ltd; Fisher Scientific; Megamations; Colonial Scientific Ltd; Boston Scientific Ltd; Thomson Micromedex; Ormed Information Systems Ltd; St. Joseph's Health System; Summit Technologies Inc; GE Medical Systems		
IWK Health	The IWK had a version update to its	Storage and access to	The IWK has permitted access or

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Centre	Health Information System (Meditech) in January, 2008. In order to complete the update the vendor requires access to the LIVE system. The IWK staff and the vendor staff partnered to work through critical system issues to ensure the update is completed successfully and to ensure on-going performance of the update. Access by the vendor (Meditech, Boston, USA) is required when providing technical support and is always done through secure dedicated connection. Access by the vendor is on request from the IWK. IWK's records indicate 181 individuals (employees and physicians) made 209 work related trips outside of Canada as reported by cost centres which funded the travel. These figures indicate the number of out of Canada trips and not potential access to personal information. In circumstances where individuals travel with laptop computers or handheld devices, most access would be to email. Remote access to other	personal information outside of Canada by service providers and partners is done either under contract with language addressing confidentiality or with the consent of the individual. Conditions or restrictions to access to personal information by employees while traveling outside of Canada are being addressed in a policy, currently being drafted in collaboration with Privacy Leads from all DHA's/IWK. While personal information is not taken by employees when traveling outside of Canada, some personal information may be accessible by employees through wireless handheld devices. When connecting to the IWK Communication system messages are	storage of personal information outside of Canada in the following circumstances: 1.The IWK has software vendors located outside of Canada who maintain systems remotely. The IWK continues to use these vendors as they provide a service which is required for continued management and operations of the health centre. (Examples – Meditech, Boston which maintains health information system; BirthNet/Spacelabs in Seattle, Washington – which maintains Fetal Archiving System; GE/Deio Anaesthesia Information System, Massachusetts; and Poison Information VDL software, California). The access to the systems is set out in written agreements and monitored by the IWK. 2.In circumstances where specialized laboratory testing is not available or cost prohibitive

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	systems containing personal information is possible. All information accessible remotely is encrypted. Contracts which provide for access/storage outside of Canada were reviewed for mitigation of access. It it was deemed that this access/storage was necessary, a confidentiality clause, secure network access and accountability were included in the contact and/or processes wherever appropriate.	encrypted while on route. In 2008, passwords became a mandatory practice on all wireless handheld devices.	in Canada, test resulting is done outside of Canada. When circumstances allow consent is obtained. Laboratory services tracks external referral lab tests. 3. When the research sponsor is located outside of Canada, no personal identifiers are provided unless consent from the patient/legal guardian has been obtained. 4. A PIA (Privacy Impact Assessment) is required when a new service is acquisitioned/implemented that requires transmittal of or access to personal information outside the country or when a vendor is a subsidiary of a U.S. based company. The PIA is reviewed by the Privacy Manager to ensure risks around disclosure of personal information is addressed. 5. Certain on-going programs which depend on treatment/patient

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
			care plans from U.S. established groups obtain patient consent prior to transmittal of personal information. An example of these programs is the Children's Oncology Group (COG).

Table 3: Summary of January 1, 2008 - December 31, 2008 Foreign Access and Storage by Universities

Universities	A (Description)	B (Conditions)	C (Reasons)
Dalhousie University	a. Service Provider for wireless products for employees	a. Mobile communications solution for employees is essential for administrative operations of the University. Significant price advantage with this service provider through the MASH sector rates negotiated by the Province.	a. Contractual security measures; restrictions on access to and disclosure of information by service provider and their employees. Internal security measures: process in place to minimize disclosure of personal information.
	b. Consulting services related to the University's planned upgrade of its internal network and systems	b. The consultant services are provided by the current provider of the systems being upgraded, and thus has the expertise to provide the services required. These systems are necessary for the operation of integral Dalhousie computing services.	b. Limited access: only where required for maintenance and troubleshooting. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.
	c. Comprehensive online tool to assist students in seeking employment	c. Providing tools for students to develop job-seeking skills is an important and necessary element of the University's student services program. This product was	c. Limited access: only where required for maintenance and troubleshooting. Contractual security measures: all personal information will be stored in Canada; restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including

Universities	A (Description)	B (Conditions)	C (Reasons)
		identified as superior in this aspect, and no similar Canadian product has been identified which provides the necessary functionality and range of services.	time restrictions, audit function, and pre-approved IP addresses.
	d. Management of access and financial processes used through the University ID Card	d. The University's identification card is used by all staff, faculty and students for a variety of purposes, including access to facilities, financial transactions on and off campus, and various administrative functions. Proper management of this integrated tool is necessary for the administrative functions of the University.	d. Limited access: only where required for maintenance and troubleshooting. Contractual security measures: all personal information will be stored in Canada; restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses; removal of personal information prior to return of hardware, where possible.
	e. Service provider for the creation of templates for various electronic financial services, e.g., purchase orders, bills, cheques, etc.	e. This is the only product offered which offers integration with the University's well-established on-line information systems, which is essential to the function of our Financial Services and Human	e. Limited access: only where required for maintenance and troubleshooting. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.

Universities	A (Description)	B (Conditions)	C (Reasons)
		Resources departments. This service provider has been used sine 2003, and offers significant price advantage to the suite of various products offered by Canadian vendors which would have to be purchased in order to achieve the same degree of program integration.	
University of King's College	Personal information about King's graduates and former students (name, address, employment, year of graduation or leaving King's, donations history and relationships) provided to contractor, Blackbaud Analytics of Charleston, South Carolina to verify addresses and conduct a wealth assessment.	King's will avoid retaining contractors that store personal information outside Canada, and will ensure personal information provided to a Canadian contractor for storage is not accessible outside Canada. King's employees traveling abroad will transport and remotely access personal information only as their duties require. Employees must take reasonable precautions to protect information transported or	Blackbaud Analytics provides this service for many Canadian universities and non-profit groups. The analysis was necessary to enable the King's Advancement Office to develop fundraising programs. King's sought legal advice before hiring Blackbaud and the contractor did not retain the information.

Universities	A (Description)	B (Conditions)	C (Reasons)
		accessed outside Canada. King's will disclose personal information outside Canada only with the consent of the person involved, where disclosure is required by law, to collect monies owing to the university, to verify drivers' licenses or motor vehicle registration or licensing, to notify relatives or friends of someone who is injured, ill or deceased, or if someone's health or safety is at risk. King's will notify the Minister of Justice of a foreign demand for disclosure of personal information.	
St Francis Xavier	a. The University's financial software "Bi-Tech" is provided by an American vendor, Sungard Bi-Tech (since 1988). This software	a. The university has taken steps to minimize our exposure to risk by restricting access to our system to designated and prescheduled time periods	a. The cost of switching software vendors is prohibitive at this time. This is a mature software product and historically access has been for semiannual updates only, therefore we have minimal exposure points.

Universities	A (Description)	B (Conditions)	C (Reasons)
	requires periodic maintenance and updates. These maintenance needs are applied to our financial software through a remote access link between our server and a “Bi-tech” server located in Chico, California. The access to our server is for software maintenance and updates *only*, it is however theoretically possible that personal information could be accessed at those times, hence this notification.	and only when maintenance and update activities cannot be accomplished by university personnel.	
	b. Established online alumni community through *imodules* in Kansas City that are based on their server. Records information	b. Information added to the server program by our alumni becomes property of StFX University and is N/A or used by any other organization. Access is	b. This database was moved to a Canadian server in April 2008.

Universities	A (Description)	B (Conditions)	C (Reasons)
	has not been provided by the university, but rather is added by individual alumni who choose to do so.	limited to graduates of Saint Francis Xavier University.	
Nova Scotia Community College	a. NSCC has allowed for the storage of personal information under their control to be held by Apply Yourself Inc., Fairfax, Virginia. Apply Yourself is an application service provider offering web-based data management for the college's online application process. Will be reviewing alternate service providers in Canada. The College will provide disclosure to electronic applicants indicating that Apply Yourself Inc is an American company and the access and use of	a. The College will provide disclosure to electronic applicants indicating that Apply Yourself, Inc., is an American company and the access and use of applications is subject to all applicable federal, state and local laws.	a. The services of Apply Yourself, Inc. are required to support the application process for many of the NSCC student applicants. There have been no emerging or known Canadian companies identified by NSCC over the past year through the usual channels – conferences, trade shows and vendor contacts. The college continues to seek on-line application solutions through products and functionality available with the NSCC current database service provider (Oracle/PeopleSoft) and products. Currently, none are ready for implementation, however, it is their understanding this solution is under development. Note: The College will allow their employees to transport personal information temporarily outside Canada but only to the extent that it is strictly necessary for their assigned duties, or as a necessary part of a research project. This information will be transported using cellular telephones, wireless handhelds, laptops and storage devices. Employees will be required to take all reasonable precautions (e.g., encryption).

Universities	A (Description)	B (Conditions)	C (Reasons)
	applications is subject to all federal, state and local laws.		Also note: For accessing personal information in College data repositories from outside Canada, the College will permit its employees to use web-based or other Internet access tools if it is a necessary part of performing his or her assigned duties or as a necessary part of a research project.
Cape Breton University	a. The University's Alumni/Donor Database, Raiser's Edge, is provided by an American vendor, Blackbaud located in South Carolina. While the software originates from Blackbaud, data is stored on servers housed at CBU. Blackbaud does also provide support service. If authorized by the University's software administrator, it is possible for the support technician to screen share site access. This access is	a. Access to systems is restricted to authorized personnel only; access occurs only for the purpose of receiving technical support that cannot be accomplished internally.	a. The University's demand for requesting technical support is minimal to non-existent from year to year. Raiser's Edge software is fulfilling the needs of the University and the cost of purchasing new software is prohibitive at this time.

Universities	A (Description)	B (Conditions)	C (Reasons)
	restricted to the screen view only and controlled by the database administrator. Once the support is concluded, access is automatically terminated. This occurred only once in 2007 for the purpose of receiving technical support. b. Approximately 65 CBU staff members traveled outside of Canada and may have (or had the ability to) access personal information via remote e-mail, Blackberry™, personal computer or by any other means. While traveling outside the country, such access is necessary for university administrators, researchers and other	b. Access to information is authorized for the purpose of required assigned duties and research.	b. Storage and access as required to meet the operational requirements of the University.

Universities	A (Description)	B (Conditions)	C (Reasons)
	employees to perform their assigned duties or as a necessary part of a research project.		
Nova Scotia Agricultural College (Note: The Laboratory Information Management System (LIMS) was reported by the Department of Agriculture)	The NSAC allows their Student Information System (SIS) provider, Datatel Inc., of Fairfax, Virginia, to provide Tier II application maintenance/support to their system, which is housed on the NSAC campus. No data resides in a foreign country. The SIS is utilized by a wide variety of stakeholders including students, staff, faculty, senior management, and various units/depts. (e.g., Financial Services, Registry, Continuing Education, Alumni Development and External Relations, Graduate Studies	Administrative rights are controlled by the NSAC Database Systems Administrator with username/password authentication for TCP/IP connectivity being granted to Datatel as required. This connectivity is restricted to a range of Datatel IP addresses. This access is monitored and compared to monthly reports provided by the vendor of the work that they have performed for the NSAC. Datatel's login information is periodically changed for security reasons and login information is only provided via direct communication via telephone to Datatel's head office.	When NSAC purchased the Datatel colleague/ Benefactor system in 2004 there were no competitors in the Canadian marketplace. All three top SIS systems were provided by US vendors – this continues to be the case. Tier II support of this type of massive integrated system is typically provided by the vendor due to the breadth and depth of knowledge required for problem resolution. The vendor has a large staff that are highly trained consultants; systems support staff and programmers who are experts on the integrated system and its many components (client software, database, programming language, systems tools, etc.). The product is also always evolving and the university needs to maintain the ongoing relationship with the vendor to take advantage of enhancement as they develop. To properly complete daily business the NSAC must continue to have Tier II support provided by this vendor.

Universities	A (Description)	B (Conditions)	C (Reasons)
	Office, Residence Services). The system houses all academic and student financial account information, as well as alumni and campaign information. The SIS is a mission critical system that supports the core business activities of the NSAC. The Datatel head office is located in Fairfax, Virginia. Datatel accesses the NSAC system on a monthly basis to solve problems that are not resolved by the NSAC first level of support which is provided by their in-house Database System Administrators. All access is via TCP/IP protocol. NSAC stakeholder access is restricted to internal NSAC network		

Universities	A (Description)	B (Conditions)	C (Reasons)
	connectivity, while Datatel access is provided through firewall security to a restricted range of Datatel IP addresses. All TCP/IP and firewall/security management is provided by the NS Provincial Resources CSU – IT Division.		

Table 4: Summary of January 1, 2008 - December 31, 2008 Foreign Access and Storage by School Boards

School Boards	A (Decision)	B (Conditions)	C (Reasons)
South Shore Regional School Board	a. The school board has contracted the services of Frontline Technologies Canada Inc. (FTC) for the scheduling and placement of substitute teachers in schools, in response to filling teacher absences. The Aesop System is an automated tool used for tracking, processing, and storing information related to teacher absences. Frontline Technologies Canada Inc. utilizes an application service provider (ASP) model for provision of the system to the School Board. The software and data reside in Toronto, Canada and the company is paid a yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone	b. The Department of Education and seven school boards have signed a five year contract with FTC that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by DOE and the School Board in writing. The following conditions exist to ensure Nova Scotia's data is protected: - Frontline has read and agreed to the provisions of the Personal Information International Disclosure Protection Act (PIIDPA) legislation. The contract also has extensive provisions for protection of personal information, including the requirement for FTC to notify DOE if they receive a foreign order or request to disclose personal information (i.e., an order pursuant to the Patriot Act or similar legislation). - Frontline Technologies Canada Inc., has contracted data centre services with SunGard Availability Services (SunGard) for housing Nova Scotia's data and the AESOP system infrastructure at their Toronto, Canada location. The School Board data is housed at the SunGard data centre and system support services are provided by FPT located in Philadelphia, USA. Data access by FPT is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and support. The	c. This solution was chosen because the software is superior to other products on the market and meets the needs of the School Board. The vendor was able to satisfy the DOE concerns regarding protection of information by agreeing to contractual requirements related to Nova Scotia privacy legislation, as well as housing the data and systems in Canada. SunGard is a high reputable and capable organization and were very cooperative in allowing the DOE to conduct an on-site audit of their facility and processes. FTC have signed off on all security and information privacy clauses in the contract, understand and agree to comply with the province's PIIDPA legislation, do not store data

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	Interactive Voice Response (IVR) system. The system is supported and maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA. There are two types of support, technical and end user. Technical support is required to ensure the system is operating as expected and available to the user community, and includes such things as performance management, data backup and recovery, and software upgrades. End user support is needed to assist the School Board with specific system problems being experienced, answer questions regarding software functionality, and provide training information and materials related to new system	following conditions apply when FPT accesses the School Board data, (i) the accesses must be logged and reported to DOE monthly (ii) access is only for the period of time required to address the issue/problem, and (iii) access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. - The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The audits are quire detailed and provide clients with an added level of confidence that SunGard are doing the right things to ensure continuance of service and protection of information. The audits encompass all areas of the organization including administrations and organization, facilities, logical access, network security, computer operations, backup and recovery processes, and change management processes. SunGard has provided the DOE with a copy of the most recent SAS70 Audit. In addition, the facility is ISO 9001:2000 certified by Lloyd's Registry Quality Assurance. - All equipment used for the Nova Scotia Aesop implementation is owned by FTC. The equipment is stored at SunGard in individual locked wire cages, and access is restricted to FTC personnel. In addition, SunGard is compliant with industry standards and best practices for data centres; including privacy of data,	in the U.S., and use secure methods for all data transmissions. Also all data accesses by employees of the parent company (Frontline Placement Technologies) are restricted to specific purposes and logged and reported to DOE monthly.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	features. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.	separate network segments, remote control cameras, raised flooring, fire detection and suppression systems, cooling, water sensors, electronic monitoring, and uninterruptible power supply systems. - Employees of FPT have signed confidentiality agreements with the company. - Only personnel authorized by the School Board will be provided access to the School Board's electronic information. - The data contained in the system is limited to that required to ensure successful operation. - An on-site audit of the SunGard data centre facility was conducted by DOE on August 27, 2008, to confirm the vendor's ability to protect school board's personal information.	
Strait Regional School Board	a. The School Board has contracted the services of Frontline Technologies Canada Inc. (FTC) for the scheduling and placement of substitute teachers in schools, in response to filling teacher absences. The Aesop System provided by FTC is an	b. The DOE and seven school boards have signed a five year contract with FTC that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by DOE and the School Board in writing. The following conditions exist to ensure Nova Scotia's data is protected: - Frontline has read and agreed to the provisions of the Personal Information International Disclosure Protection	c. This solution was chosen because the software is superior to other products on the market and meets the needs of the School Board. The vendor was able to satisfy the DOE concerns regarding protection of information by agreeing to

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	automated tool used for tracking, processing, and storing information related to teacher absences. Frontline Technologies Canada Inc. utilizes an application service provider (ASP) model for provision of the system to the School Board. The software and data reside in Toronto, Canada and the company is paid a yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. FPT is located in Philadelphia, USA. There are two types of support, technical and end user. Technical support is required to ensure the system is operating as expected and available to	Act (PIIDPA) legislation. The contract also has extensive provisions for protection of personal information, including the requirement for FTC to notify DOE if they receive a foreign order or request to disclose personal information (i.e., an order pursuant to the Patriot Act or similar legislation). - Frontline Technologies Canada Inc. has contracted data centre services with SunGard Availability Services (SunGard) for housing Nova Scotia's data and the Aesop system infrastructure at their Toronto, Canada location. The School Board data is housed at the SunGard data centre and system support services are provided by FPT located in Philadelphia, USA. Data access by FPT is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and support. The following conditions apply when FPT accesses the School Board data (i) the accesses must be logged and reported to DOE monthly; (ii) access is only for the period of time required to address the issue/problem, and (iii) access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. - The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The audits are quite detailed and provide	contractual requirements related to Nova Scotia privacy legislation, as well as housing the data and systems in Canada. SunGard is a highly reputable and capable organization and were very cooperative in allowing the DOE to conduct an on-site audit of their facility and processes. FTC have signed off on all security and information privacy clauses in the contract, understand and agree to comply with the province's PIIDPA legislation, do not store data in the U.S., and use secure methods for all data transmissions. Also all data accesses by employees of the parent company (Frontline Placement Technologies) are restricted to specific purposes and logged and reported to DOE monthly.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	the user community, and includes such things as performance management, data backup and recovery, and software upgrades. End user support is needed to assist the School Board with specific system problems being experienced, answer questions regarding software functionality, and provide training information and materials related to new system features. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.	clients with an added level of confidence that SunGard are doing the right things to ensure continuance of service and protection of information. The audits encompass all areas of the organization including administration and organization, facilities, logical access, network security, computer operations, backup and recovery processes, and change management processes. SunGard has provided the DOE with a copy of the most recent SAS70 audit. In addition, the facility is ISO 9001:2000 certified by Lloyd's Registry Quality Assurance. - All equipment used for the Nova Scotia Aesop implementation is owned by FTC. The equipment is stored at SunGard in individual locked wire cages, and access is restricted to FTC personnel. In addition, SunGard is compliant with industry standards and best practices for data centres; including privacy of data, separate network segments, remote control cameras, raised flooring, fire detection and suppression systems, cooling, water sensors, electronic monitoring, and uninterruptible power supply systems. - Employees of FPT have signed confidentiality agreements with the company. - Only personnel authorized by the School Board will be provided access to the School Board's electronic information.	

School Boards	A (Decision)	B (Conditions)	C (Reasons)
		- The data contained in the system is limited to that required to ensure successful operation. - An on-site audit of the SunGard centre facility was conducted by DOE on August 27, 2008, to confirm the vendor's ability to protect school board's personal information.	
Halifax Regional School Board	a. Ten (10) staff members traveled outside Canada, which would have had access to personal information via their Blackberries™. b. The School Board has contracted the services of Frontline Technologies Canada Inc. (FTC) for the scheduling and placement of substitute teachers in schools, in response to filling teacher absences. The Aesop System provided by FTC is an automated tool used for tracking, processing, and storing information related	a. Relevant HRSB policies would apply to Blackberry™ usage outside of Canada. Each to Blackberry™ is password protected. The HRSB will incorporate into its policy direction on access and storage of personal information outside of Canada. b. The DOE and seven school boards have signed a five year contract with FTC that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by DOE and the School Board in writing. The following conditions exist to ensure Nova Scotia's data is protected: - Frontline has read and agreed to the provisions of the *Personal Information International Disclosure Protection Act* (PIIDPA) legislation. The contract also has extensive provisions for protection of personal information, including the requirement for FTC to notify	a. The staff members at issue occupy management positions and must be available by e-mail for decision making and information purposes. b. This solution was chosen because the software is superior to other products on the market and meets the needs of the School Board. The vendor was able to satisfy the DOE concerns regarding protection of information by agreeing to contractual requirements related to Nova Scotia privacy legislation, as well as housing the data and systems in Canada.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	to teacher absences. Frontline Technologies Canada Inc. utilizes an application service provider (ASP) model for provision of the system to the School Board. The software and data reside in Toronto, Canada and the company is paid a yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. FPT is located in Philadelphia, USA. There are two types of support, technical and end user. Technical support is required to ensure the system is operating as expected and available to the user community, and includes such things as performance management,	DOE if they receive a foreign order or request to disclose personal information (i.e., an order pursuant to the *Patriot Act* or similar legislation). - Frontline Technologies Canada Inc. has contracted data centre services with SunGard Availability Services (SunGard) for housing Nova Scotia's data and the Aesop system infrastructure at their Toronto, Canada location. The School Board data is housed at the SunGard data centre and system support services are provided by FPT located in Philadelphia, USA. Data access by FPT is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and support. The following conditions apply when FPT accesses the School Board data (i) the accesses must be logged and reported to DOE monthly; (ii) access is only for the period of time required to address the issue/problem, and (iii) access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. - The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The audits are quite detailed and provide clients with an added level of confidence that SunGard are doing the right things to ensure continuance of service and protection of information. The audits encompass all areas of the organization including	SunGard is a high reputable and capable organization and were very cooperative in allowing the DOE to conduct an on-site audit of their facility and processes. FTC have signed off on all security and information privacy clauses in the contract, understand and agree to comply with the province's PIIDPA legislation, do not store data in the U.S., and use secure methods for all data transmissions. Also all data accesses by employees of the parent company (Frontline Placement Technologies) are restricted to specific purposes and logged and reported to DOE monthly.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	data backup and recovery, and software upgrades. End user support is needed to assist the School Board with specific system problems being experienced, answer questions regarding software functionality, and provide training information and materials related to new system features. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.	administration and organization, facilities, logical access, network security, computer operations, backup and recovery processes, and change management processes. SunGard has provided the DOE with a copy of the most recent SAS70 audit. In addition, the facility is ISO 9001:2000 certified by Lloyd's Registry Quality Assurance. - All equipment used for the Nova Scotia Aesop implementation is owned by FTC. The equipment is stored at SunGard in individual locked wire cages, and access is restricted to FTC personnel. In addition, SunGard is compliant with industry standards and best practices for data centres; including privacy of data, separate network segments, remote control cameras, raised flooring, fire detection and suppression systems, cooling, water sensors, electronic monitoring, and uninterruptible power supply systems. - Employees of FPT have signed confidentiality agreements with the company. - Only personnel authorized by the School Board will be provided access to the School Board's electronic information. - The data contained in the system is limited to that required to ensure successful operation.	

School Boards	A (Decision)	B (Conditions)	C (Reasons)
		- An on-site audit of the SunGard centre facility was conducted by DOE on August 27, 2008, to confirm the vendor's ability to protect school board's personal information.	
Tri-Country Regional School Board	The School Board has contracted the services of Frontline Technologies Canada Inc. (FTC) for the scheduling and placement of substitute teachers in schools, in response to filling teacher absences. The Aesop System provided by FTC is an automated tool used for tracking, processing, and storing information related to teacher absences. Frontline Technologies Canada Inc., utilizes and application service provider (ASP) model for provision of the system to the School Board. The software and data reside in Toronto, Canada and the company is paid a	The DOE and seven school boards have signed a five year contract with FTC that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by DOE and the School Board in writing. The following conditions exist to ensure Nova Scotia's data is protected: - Frontline has read and agreed to the provisions of the Personal Information International Disclosure Protection Act (PIIDPA) legislation. The contract also has extensive provisions for protection of personal information, including the requirement for FTC to notify DOE if they receive a foreign order or request to disclose personal information (i.e., an order pursuant to the Patriot Act or similar legislation). - Frontline Technologies Canada Inc. has contracted data centre services with SunGard Availability Services (SunGard) for housing Nova Scotia's data and the Aesop system infrastructure at their Toronto, Canada location. The School Board data is housed at the SunGard data centre and system support services are	This solution was chosen because the software is superior to other products on the market and meets the needs of the School Board. The vendor was able to satisfy the DOE concerns regarding protection of information by agreeing to contractual requirements related to Nova Scotia privacy legislation, as well as housing the data and systems in Canada. SunGard is a high reputable and capable organization and were very cooperative in allowing the DOE to conduct an on-site audit of their facility and processes. FTC have signed off on all security and information privacy clauses in the

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. FPT is located in Philadelphia, USA. There are two types of support, technical and end user. Technical support is required to ensure the system is operating as expected and available to the user community, and includes such things as performance management, data backup and recovery, and software upgrades. End user support is needed to assist the School Board with specific system problems being experienced, answer questions regarding software functionality, and provide training information and materials	provided by FPT located in Philadelphia, USA. Data access by FPT is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and support. The following conditions apply when FPT accesses the School Board data (i) the accesses must be logged and reported to DOE monthly; (ii) access is only for the period of time required to address the issue/problem, and (iii) access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. - The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The audits are quite detailed and provide clients with an added level of confidence that SunGard are doing the right things to ensure continuance of service and protection of information. The audits encompass all areas of the organization including administration and organization, facilities, logical access, network security, computer operations, backup and recovery processes, and change management processes. SunGard has provided the DOE with a copy of the most recent SAS70 audit. In addition, the facility is ISO 9002:2000 certified by Lloyd's Registry Quality Assurance. - All equipment used for the Nova Scotia Aesop	contract, understand and agree to comply with the province's PIIDPA legislation, do not store data in the U.S., and use secure methods for all data transmissions. Also all data accesses by employees of the parent company (Frontline Placement Technologies) are restricted to specific purposes and logged and reported to DOE monthly.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	related to new system features. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.	implementation is owned by FTC. The equipment is stored at SunGard in individual locked wire cages, and access is restricted to FTC personnel. In addition, SunGard is compliant with industry standards and best practices for data centres; including privacy of data, separate network segments, remote control cameras, raised flooring, fire detection and suppression systems, cooling, water sensors, electronic monitoring, and uninterruptible power supply systems. - Employees of FPT have signed confidentiality agreements with the company. - Only personnel authorized by the School Board will be provided access to the School Board's electronic information. - The data contained in the system is limited to that required to ensure successful operation. - An on-site audit of the SunGard centre facility was conducted by DOE on August 27, 2008, to confirm the vendor's ability to protect school board's personal information.	

Table 5 - Summary of January 1, 2008 – December 31, 2008 Foreign Access and Storage by Municipalities[2]

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
Halifax Regional Municipality	Between January 1 and December 31, 2008, two hundred and forty seven (247) HRM staff traveled outside of Canada and had the ability to access personal information via one or more of the following means: cell phone, Blackberry, laptop, memory stick, VPN.	Prior to traveling, staff was advised that HRM communication tools (cell phones, blackberries, laptops, memory sticks, VPN) were to be password protected.	The HRM staff, who were approved for traveling outside of Canada with their communication device(s), were expected to maintain a means of communication with their respective staff/Business Unit in order to fulfill operational responsibilities/requirements.
Municipality of the County of Kings	One staff member traveled outside Canada during the reporting period and had the ability to access his personal e-mail on his corporate Blackberry.	Access was limited to e-mail use on his corporate e-mail account.	Remote access is protected by username/password authentication, and is delivered over an encrypted link.
NS Association of Regional Development Authorities (NSARDA)	For operational reasons – storage, MSARDA allowed	The information is not to sell, disclose and/or be used for any	There was no local or domestic provider of this specific database and service and therefore it was necessary to host the information at source. This was agreed by the

[2] Municipalities of the Counties of Annapolis, East Hants, Pictou and West Hants, and the Towns of Antigonish, Amherst, Digby, Liverpool, Lunenburg, Shelburne, Westville and Wolfville had no access or storage outside of Canada to report.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	storage of a Business Retention and Expansion database be located outside of Canada. The licensing agreement is with NSARDA. The system is a legacy system.	purpose. The information is only stored outside of Canada.	NSARDA Executive for the Business Retention and Expansion Program.
Municipality of the County of Colchester	Five staff members traveled outside Canada during calendar 2008 and could have accessed personal e-mail or stored information and e-mail through GroupWise, via a laptop or Blackberry.	Employees have been notified to limit e-mail use with blackberry's and laptops during time out of the country unless absolutely necessary. Currently in the process of creating a new e-mail policy that will require employees to limit any personal information being sent while visiting/working outside of Canada.	When staff is traveling for business or personal reasons, they are expected to monitor their business e-mail in order to fulfill their job responsibilities.