Nova Scotia Personal Information International Disclosure Protection Act

2009 Annual Report

NS Information Access and Privacy Office

Message from the Minister of Justice

I am pleased to provide the fourth 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 and municipal entities are required to report the decision and description of any foreign access and storage of personal information occurring from January 1, 2009 to December 31, 2009 to the Minster of Justice. This report is based on the PIIDPA reports received by the Department of Justice.

This report contains a summary of the 53 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: 26 entities reported that there was no access or storage outside of Canada for the 2009 calendar year.

Original signed by

_____

The 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, 2009 – December 31, 2009 Foreign Access and Storage by Government Departments[1]

Department	A (Description)	B (Conditions)	C (Reasons)
Community Services	**1. Application Support.** Since 2002, the Nova Scotia Housing Development Corporation has contracted Yardi Systems, Inc. under an alternate services provider (ASP) agreement to provide Tier II application support and maintenance as well as to manage the application hardware configuration necessary to operate the application. Tier II application support is provided by the Yardi Canadian offices operated in Mississauga, Ontario once issues reported are vetted by Housing Authority IT staff. The data is stored on database servers located at a Data Centre in Mississauga, Ontario operated by Q9 Networks. The application and database servers are managed by the Yardi Systems ASP Group located in Santa Barbara, California. This access is ongoing in order to ensure the ongoing operation and efficient	**1. Application Support.** Under the terms of the contract, Yardi agrees that it will not use, disseminate or in any way disclose any of the confidential information of the Nova Scotia Housing Development Corporation to any person, firm or business except to the extent it is necessary to perform its obligations or exercise it rights.	**1. Application Support.** Before entering into this arrangement, staff from the Housing Authorities (an agent of the Nova Scotia Housing Development Corporation) and the NS Department of Community Services underwent an RFP process and through a structured evaluation process of the proposals received, determined that the Yardi Systems software operated under an ASP agreement was the best solution. The software provided the best business functionality based on criteria defined at the time of the RFP process for the costs proposed. The technical framework proposed to operate this software was deemed acceptable based on criteria defined at the time of the RFP process for the costs proposed.

1

Department	A (Description)	B (Conditions)	C (Reasons)
	performance of the server environment and the Yardi Voyager application, itself, and minimize service disruptions to Housing Authority users. This group is also responsible for applying operating system patches and system upgrades as required. **2. <u>Residential Treatment Facilities.</u>** Children In Care of the Minister of Community Services may require treatment services that are not available in the Province of Nova Scotia and on occasion within Canada. During the 2009 calendar year, six children in care were placed in residential treatment facilities in the state of Utah to receive residential treatment services. As part of the referral for placement to a treatment facility, information concerning the child, any medical diagnosis, treatment needs and relevant family information is shared with the placing facility. This information is provided to ensure that the facility will be able to meet the child's	**2. <u>Residential Treatment Facilities.</u>** Information provided in these situations is to be used solely for the purpose of the determination of placement and the development of treatment plans for children.	**2. <u>Residential Treatment Facilities.</u>** Information provided to the placing facility is stored in accordance with the Health Insurance Portability and Accountability Act (HIPPA) of 1996. The information is stored in a locked environment on the facility campus for a period of not more than six years, or until the client reaches the age of 22, whichever is the longest. Information is released only with a written request by the legal guardian or client, when the client has reached the age of 18 years.

Department	A (Description)	B (Conditions)	C (Reasons)
	clinical needs, and for the purpose of developing an appropriate treatment plan for the child. Information provided to the placing facility would include electronic information such as e-mails with agency social workers in Nova Scotia, and paper copies of the information identified above.		
Education	**1. <u>NS Provincial Library – Integrated Library System</u>** Nova Scotia Provincial Library (NSPL) maintains an integrated library system (ILS) on a cost-recovery basis for a consortium consisting of 64 branch libraries in eight regional library systems, and four government department libraries. The ILS provides a library	**1. <u>NS Provincial Library – Integrated Library System</u>** 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	**1. <u>NS Provincial Library – Integrated Library System</u>** The decision was made to continue to 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

Department	A (Description)	B (Conditions)	C (Reasons)
	catalogue, a purchasing module, and a circulation module (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 and email address. This personal information is voluntarily given when a client registers for a library card. Attached to the clients' account number are titles currently on loan to the individual, those for which the individual has been billed and/or has paid, and those which the user has requested. Transaction logs, maintained at NS Provincial Library, DOE, are retained for 3 months. The ILS is owned by an American Company, SirsiDynix, and access to	staff must be contacted when the company requires access to the ILS server. NSPL enables 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 technologically possible.	2003, the company was a Canadian 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)
	personal client information from outside Canada is possible with SirsiDynix. There is no Canadian vendor which supplies a similar product. **2. <u>Remote Email Access</u>.** A number of Department of Education staff traveled outside Canada and had the ability to access personal information contained in email or stored in GroupWise email system, using devices such as the BlackBerry and laptops.		
Finance	**1. <u>Travel.</u>** It was necessary for 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.	**1. <u>Travel.</u>** 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 transaction to SAP systems is permitted without the knowledge and	**1. <u>Travel.</u>** 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.

Department	A (Description)	B (Conditions)	C (Reasons)
	2. <u>Remote Access</u>. 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 SAPs own secure internal support network and carried out by SAP staff resident in SAP service locations such as the United States, Ireland, Brazil, Germany and India. This remote access very rarely involves access of personal information, but in cases where access does involve potential access to personal information for the purposes of resolving a specific support problem, records and audit logs of that access are maintained.	approval of Division management. **2. <u>Remote Access</u>.** When SAP Support Staff have reason to access any of the Province's SAP systems as a part of problem remediation, all production system transaction access is approved by 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.	**2. <u>Remote Access</u>.** 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 CIS 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 remove the need for 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.
Health	**1. <u>Storage.</u>** There were no approvals granted for the storage of		

Department	A (Description)	B (Conditions)	C (Reasons)
	personal information in the custody or control of the Department. The Department granted the following approvals for access to personal information in the custody or control of the Department outside of Canada: **2. Relay Health.** McKesson Canada, operator of the Department of Health HealthLink 811, partnered with Relay Health to develop their Telecare application. As a result, Relay Health provides third level technical support for the information technology application that enables HealthLink 811 operations. In cases where third level technical support is needed for the Telecare application, Relay Health, a US-based company, will require remote access to the CECC which contains personal information from outside of Canada.	**2. Relay Health.** Access is temporary and only utilized when required after IT support, at the work station and levels through the call centre, are unable to resolve. To ensure the security of personal information, access is granted through a secure VPN. Access will be granted to the Implementation Engineer, the Development Team or the 24 hour Technical Support Analyst as required. While access to the CECC means Relay Health have access to personal information stored in Canada, the scope and focus of access rights will be limited to the source code of the application. Policies and procedures dictate that at no time	**2. Relay Health.** McKesson Canada's partner in the development of the Teletriage application is Relay Health. As a result, Relay Health is the only available provider of third level technical support for the information technology application that enables HealthLink811 operations.

Department	A (Description)	B (Conditions)	C (Reasons)
		shall Relay Health download or copy information from the CECC. The CECC is monitored by McKesson and all downloads and print activities are captured through the change control system employed by McKesson. As well, employees of Relay Health, under the umbrella of McKesson Corporation, are bound by the Corporate Code of Conduct.	
	3. Language Line Services. Language Line Services was subcontracted by McKesson Canada to provide telephone based language interpreter services for callers whose first language is not English. Language Line Services are provided by multiple sources across North America. Access to personal information is granted through obtaining consent from the caller to engage third party interpretation services to facilitate the call in the caller's language of choice. **4. Employee Access.** During the	**3. Language Line Services.** Interpreter service is provided over the phone. Language Line services, as per McKesson Canada's policy requirements, do not result in downloading, printing or documentation of personal information. Interpreters trained in language interpretation are the only representatives who have access to personal information throughout the encounter.	**3. Language Line Services.** McKesson Canada has entered into a partnership with Language Line Services to meet contractual requirements for the provision of culturally safe care and improving access to primary health care services for all Nova Scotians. This third party interpretation service is required to address linguistic barriers. McKesson Canada identified they would be unable to meet the service level standards outlined in the contract if they used the known Canadian service – CanTalk.

Department	A (Description)	B (Conditions)	C (Reasons)
	period, 16 Department staff 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.	**4. Employee Access.** The Department's Transmission of Confidential Information by E-mail or Fax Guideline (2004) prohibits the inclusion of personal information in e-mail 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 the e-mail within the GroupWise system. Therefore, the amount of personal information held or sent by e-mail and available for access while staff were outside the country should be limited.	**4. Employee Access.** When staff travel 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.

Health Promotion and Protection	**1. <u>Storage</u>.** There was no storage of personal information in the custody or control of the Department of Health Promotion and Protection outside of Canada. **2. <u>Employee Access</u>.** Four staff members outside Canada on business had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise system.	**2. <u>Employee Access</u>.** The Department's Transmission of Confidentiality Information by E-Mail and Fax Guideline (2004) prohibits the inclusion of personal information in e-mail 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 within the GroupWise system. Therefore, the amount of personal information held or sent by e-mail and available for access while staff were outside the country should be limited.	**2. <u>Employee Access</u>.** When staff travel 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.

Information Management	Symphony Services, located in California, was awarded a contract in 2006 by the Province of Nova Scotia (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 the Chief Information Office pursuant to subsection 5(3) of the Personal Information International Disclosure Protection Act ("PIIDPA"), with respect to the award of the contract to Symphony Services in 2006. PNS subsequently renewed the contract in 2009 to permit Symphony Services to continue to provide support services for EMS. In the course of providing services, 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	Microsoft's Terminal Services allows Symphony Services to view the PNS database used by EMS to store personal information. However, it does not give Symphony Services the ability to remove or copy any files. Once Symphony Services' work is completed, its access to the database is disabled by PNS and is only re-enabled by PNS during scheduled support services or troubleshooting work. Under the agreement with PNS, Symphony Services covenants that it will comply with its obligations as a service provider under PIIDPA and will strictly enforce the security arrangements required to protect personal information to which it has access. Symphony Services is also required to confirm the details of those security requirements upon receipt of a request to do so from PNS. PNS employees may at any time travel to the offices of Symphony Services to inspect the security measures it has put in place to	The EMS solution was selected by PNS because Symphony Services was very familiar with the PNS telephone billing requirements (it had previously supplied both Tru Server and TIMS). Symphony Services has successfully migrated PNS data from Tru Services to EMS and its prior experience lowered the risk associated with the migration of data. There is currently no alternative method of support access for EMS within Canada.

	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. There are times when Canadian-based Manufacturer technical support services cannot resolve a technical issue and have to raise the issue with the Manufacturer's technical support organization. This would be the Manufacturer's staff who actually develop/provide worldwide support of the product. This is usually US-based, but can be in any country. An example of this is Novell GroupWise. Our support comes from Novell Canada support services. If this Canadian support cannot correct an issue with GroupWise, we would allow a PC to be controlled from the US-based Novell support and the PC screen would be monitored by Government internal resources.	protect such personal information. The connection to remote control a PC must be initiated by both sides of the connection. Internal support does not leave the terminal while external support is working on the solution. The remote connection does not allow external support to transfer any data remotely. This allows internal support the options to disconnect the link and see every step that the non-Canadian Manufacturer support end services takes in order to resolve the problem. If any system data, not personal data, is required to be sent, it will be sent through a secure encrypted channel.	This generic method of external support will: 1. Not allow the transfer of personal information over the connection. 2. Connectivity will only be enabled upon connection initiation from both sides. No connectivity is automated. It is set up from a phone call between internal and remote access support and agreement of work to be performed. The connection will not be automatically available for any reason. 3. Transfer of any system information will be performed

	Personnel files are not transferred outside Canada, but Novell remote support would be given access to system files, not personal files, in order to correct the problem.		through a secure encrypted methodology. Personal information is not to be sent.
Intergovern-mental Affairs	**1. Iron Mountain.** In 2006, the Department 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 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.	**1. Iron Mountain.** The service contract with Iron Mountain states: 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 in the manner contemplated by the agreement. Iron Mountain shall use the same degree of care to safeguard the Confidential Information of Intergovernmental Affairs as it utilizes to safeguard its own Confidential Information. All devices which travel out of country are password protected.	**1. Iron Mountain.** The decision was made to use Iron Mountain 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. In March of 2010 Intergovernmental Affairs revised its STOR retention schedule to include more appropriate dispositions and longer semi-active storage periods. This will enable the records currently held at Iron Mountain to be re-classified so that the Provincial Government Records Centre will accept them and the contract with Iron Mountain can be closed. Intergovernmental Affairs intends to action this in 2010.

	2. Travel. Staff routinely take electronic devices including Blackberries, Laptop computers and Netbooks which may store and/or access personal information.	**2. Travel.** Blackberries can have their memory remotely wiped and staff have been briefed on the process on how to have the device wiped. Laptops and Netbooks taken out of country do not store personal information, but only access it from servers in Canada. The connection to that information is again password protected.	**2. Travel.** Staff need to be able to take electronic devices so that they are able to communicate with our offices and receive important information while supporting senior officials. These devices need contact information contained within them so that they are able to request information from the relevant stakeholders.
Justice	**1. All Divisions.** For 2009, there were 12 employees who traveled outside Canada and may have accessed personal information through email or personal computer during that time. **2. Legal Services**, under the Child Abduction Act, c. 67, R.S.N.S., 1989, implemented the Hague Abduction Convention. Personal information relating to parents, grandparents and children was shared with Agency Authority (Washington) in USA and child protection agency in Georgia for court application.	**1. All Divisions.** Remote access to GroupWise is protected by username/password authentication and is delivered over an SSL-encrypted link via the secure Blackberry GroupWise server. **2. Legal Services.** Restrictions or conditions as per Hague Abduction Convention.	**1. All Divisions.** When staff travel, they are sometimes expected to monitor their e-mail or conduct business for operational purposes. **2. Legal Services**. Child Protection Group at DOJ required to disclose information as part of the duty imposed by the Convention for Nova Scotia for court application.

	3. <u>Correctional Services</u>. JEMTEC Inc. was the best choice to provide <u>Electronic Supervision of Offenders</u> monitoring and services to Nova Scotia and as such 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 subcontractors, which include BI Inc. and Omnilink Inc - located in Toronto, Canada, Boulder, Colorado, US and Alpharetta, Georgia, US respectively.	**3. <u>Correctional Services.</u>** The restrictions included: 3a. JEMTECS' 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. 3b. JEMTECS' Project Manager shall immediately notify DOJ of all relevant details of any unauthorized access. JEMTECS' 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. JEMTECS' Project Manager shall verify what steps have been taken to prevent further unauthorized access. 3c. The systems contain a native journal function to allow system and program management users access to an audit trail of all changes made to an individual's	**3. <u>Correctional Services.</u>** 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 to ensure mission critical operation of the system.

		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 these 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.	
	4. Correctional Services. JEMTEC Inc. was awarded the contract for Voice Verification of Offenders. All personal information is stored in a secure database located in secure Monitoring Centres owned/ operated by JEMTEC (including it's subcontracted monitoring services), BI and Biometric Securities, located in Toronto, Canada, Boulder, Colorado and	4a. JEMTECS' 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. 4b. Only JEMTEC Inc. and DOJ personnel designated by DOJ shall have 'permanent' user	4. 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

	Decatur, Georgia US respectively.	access to the host monitoring system. JEMTECS' Project Manager shall immediately notify DOJ of all relevant details of any unauthorized access to the host monitoring system. JEMTECS' Project Manager shall immediately notify DOJ of all relevant details of any unauthorized access. JEMTECS' Project Manager shall document the reason the access occurred, the person/ agency that accessed the information and the time, date, specific data compromised and duration of the access. JEMTECS' Project Manager shall verify what steps have been taken to prevent further unauthorized access. 4c. The VoiceID system contains a native journal function 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	operation of the system

		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.	
	5. Iron Mountain. In July 2004, the Department of Justice entered into a service contract with Iron Mountain Canada Corporation to provide document destruction and government record storage. In 2005, the Department of Justice reviewed the physical and procedural security and access environment at Iron Mountain Canada Corporation in Hammonds Plains.	**5.** Information held in a confidential and secure manner as outlined in agreement with Iron Mountain.	**5.** The Department of Justice entered into this contract as there was insufficient storage available at the Records Centre.

Labour and Workforce Development	Labour & Workforce Development (LWD) utilizes NRSPro.com (formerly GEDScoring.com) for the purpose of storing and processing information in support of the General Educational Development (GED) Program. The GED is composed of a series of five tests that evaluate participants' skills in the areas of language arts-reading, language arts-writing, math, social studies and science. An internationally recognized assessment tool of high school equivalency, GED credential is accepted by employers across NS and Canada and serves an important function in labour mobility. Approximately 1,500 tests are conducted each year in NS. LWD scans the test sheets locally and sends data to NRSPro via an encrypted secure sockets layer (SSL) connection. Test scoring is completed remotely by NRSPro, with test results and certificates transmitted via SSL connection to LWD for printing. Test results and certificates may be viewed on a password protected NRSPro website by authorized LWD staff.	LWD has a contract with NRSPro which stipulates that all information will be kept private and confidential and will not be released to any third party without written authorization from the department. The contract also states that only personnel authorized by LWD will be provided access to store and retrieve NS information.	There are only two vendors, both located in the USA, certified by GEDTS to conduct test scoring that were felt to be able to handle Canadian requirements. At the present time, there is no option of a software solution with data storage in Canada. The option of developing an in-house customized system to manage the GED Program has not been chosen due to cost and time constraints which would result in an interruption in client service to allow for design development, and certification from GEDTS. NRSPro provides instant scoring, immediate reporting times, detailed reports, incorporating NS forms and letters as report options and allows students and verifiers to get instant results online.

	The data is then stored in an NRSPro database located in Spanish Fork, Utah, USA for processing and as a record for future reference. Storage is required for students re-writing tests. In the event that we terminate services with NRSPro, the data will be returned/transferred to LWD or another service provider, and securely removed from the NRSPro database. Information is also transferred, by NRSPro, to the General Educational Development Testing Services (GEDTS) international database. GEDTS is located in Washington DC, with the database maintained by Marsys, located in Miami, Florida, USA with a backup database in San Mateo, California, USA. The international database was established in support of the GED Program and it is mandatory that all jurisdictions send data to GEDTS as part of the GED licensing agreement. Personal information collected in the GEDTS international database is used for statistical reporting by jurisdiction.		

Natural Resources	**1. <u>Storage.</u>** There was no storage of personal information in the custody or control of the Department of Natural Resources outside of Canada. **2a. <u>Remote Access - Business</u>**. Staff members who traveled outside Canada on business may have had the ability to access personal information via remote e-mail, Blackberry, personal computer or by any other means. **2b. <u>Remote Access - Pleasure</u>**. Staff members who traveled outside Canada on pleasure may have had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to GroupWise email system. **3. <u>Off site record storage</u>** contracted with Iron Mountain Canada (subsidiary of the American Company)	**2a. <u>Remote Access - Business</u>**. Remote access to Group Wise is protected by username/password authentication and is delivered over an SSL-encrypted link via the secure Blackberry GroupWise server. **2b. <u>Remote Access - Pleasure</u>**. Remote access to Group Wise is protected by username/password authentication, and is delivered over an SSL encrypted link. **3. <u>Off site record storage.</u>** Iron Mountain is to safeguard and maintain protected storage of the Departments Records. Iron Mountain Canada Corporation confirms that personal information is maintained and disclosed in accordance with our contractual arrangement in	**2a. <u>Remote Access - Business</u>**. When staff travel for business reasons, they are expected to monitor their email and voice mail for business continuity purposes. **2 b. <u>Remote Access - Pleasure</u>**. When staff travel for pleasure, they may be required to maintain contact with operations. **3. <u>Off site record storage</u>** .Off site storage of backup 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.

		compliance with all applicable privacy legislation.	
Public Prosecution Service	**1. <u>Storage</u>**. There was no storage of personal information outside Canada by the Public Prosecution Service. **2. <u>Travel.</u>** There was access to personal information using wireless data devices, including BlackBerrys and laptops on a daily basis while staff were visiting countries outside of Canada. The locations of the access were: Illinois, Florida, Hawaii, Maine, Massachusetts, New York and New Hampshire in the United States. Access was also made from Finland, States of the Russian Federation, Spain and Germany.	**2. <u>Travel.</u>** The conditions placed on access involved use of encryption and password protection.	**2. <u>Travel.</u>** Access was granted in order to permit staff to discharge some of their responsibilities while absent from their offices.
Service NS and Municipal Relations	**1. The <u>Interprovincial Record Exchange</u>** is a system that allows Canadian motor vehicle jurisdictions to securely query other jurisdiction's driver and vehicle records. The Canadian Council of Motor Transport Administrators (CCMTA) acts as the clearing house and administrators for this	**1. <u>Interprovincial Record Exchange.</u>** 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-	**1. <u>Interprovincial Record Exchange.</u>** 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, and infractions occurring is another jurisdiction are recorded on the driver's record in Nova Scotia.

	system, and operates the secure network over which it runs. A partnership arrangement now exists with the American Association of Motor Vehicle Administrators (AAMVA) to extend the system to the US. **2. <u>Travel</u>**. Nine SNSMR staff traveled outside Canada for a total of 18 trips during the reporting period and accessed GroupWise email from a laptop or Blackberry while away. **3. <u>Credit card transaction information</u>** resulting from payments for on-line services through ACOL or SNSMR, in-person services at Access Centers, Land Registration Offices, and the Business Registration Unit, or mail-in services is subject to transborder data flow through US based credit card processing services for payment authorization and account reconciliation. Personal information that is transmitted through or stored in the US is at risk of a foreign demand for disclosure under the *Patriot Act.*	formatted and specific as to what information is displayed. CCMTA has contracts with each of its member jurisdictions that conform to the jurisdiction's privacy legislation concerning disclosure and consent. **2. <u>Travel</u>**. Remote access to GroupWise is protected by Username/Password authentication and is delivered over an SSL encrypted link. **3. <u>Credit card transaction information</u>**. All service providers in the credit card payment chain are subject to strict security precautions to protect credit card information from unauthorized or accidental disclosure. The service providers are Payment Card Industry - Data Security Standards (PCI-DSS) certified and must also follow terms and conditions as defined by the card issuing institutions. Cardholders have agreed to the card issuing institutions' privacy statements	**2. <u>Travel</u>**. Maintain contact with operations. **3. <u>Credit card transaction information.</u>** SNSMR offers credit card payments as a convenience for customers and to provide efficient and effective on-line services to clients.

	4. <u>Photo Licence/ID</u>. L-1 Identity Solutions (Formerly Digimarc) of Billerica, MA was awarded the contract to provide Photo License/Photo ID equipment, software integration and support services for the Registry of Motor Vehicles in 1999. The current contract expires in 2010 and will be replaced with a new contract under the joint Atlantic Canada Photo License Project. One component of the system, the Photo License database server that stores client photos, digitized signatures, personal information and Driver Master Number is located at the Provincial Data Center. In 2006, two Digimarc support technicians in Fort Wayne were provided remote access via VPN to the database server in order to provide tier II/III support. Routine maintenance and support for this system is provided by a local L-1 field technician, with the Billerica technicians acting as back-up, or	that include a notice that third-party service providers may be used to process credit card transactions. **4. <u>Photo Licence/ID</u>**. Access from the Billerica location is restricted via VPN username/password to these two support technicians and on the database server by the privileged account username/password. Access will be in response to escalated support calls only.	**4. <u>Photo Licence/ID</u>**. Access by L-1 Identity Solutions in Billerica is an operational requirement in response to Photo License/Photo ID outages that affect the delivery of customer service.

	managing escalated problems that the local technician isn't able to resolve.		
Tourism, Culture and Heritage	**1. <u>Mail</u>.** The department has contracted Cloutier Direct Inc. (CDI) of Scarborough, Maine to mail Nova Scotia tourism information to potential visitors from the U.S. and other countries. The requests are received through our customer contact centre/call centre which is located in Halifax, through the Novascotia.com website and through regular mail. On a daily basis, CDI downloads U.S. and international requests from our contact centre and mails out the requested information. **2. <u>Vital Stats Online</u>.** Decision to allow primary service provider (Unisys Canada Inc.) for Internet resource NOVA SCOTIA HISTORICAL VITAL STATISTICS ONLINE (NSHVSO) operated by NS Tourism, Culture and Heritage (Archives and Records Management Division), to outsource to service.	**1. <u>Mail</u>.** 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. **2. <u>Vital Stats Online</u>.** No disclosure to, or retention of credit card personal information by service sub-provider outside Canada except as required to carry out and verify online commercial transactions with NSHVSO service clients.	**1. <u>Mail</u>.** 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. We require the use of this company as the information resides in the U.S. **2. <u>Vital Stats Online</u>.** 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 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

	3. <u>Facebook/Twitter.</u> Description of each decision made during the above-noted calendar year to allow storage or access outside Canada of personal information in the custody or under the control of the public body: Decision to launch and maintain a Facebook page, titled "Nova Scotia Museum". Contents on page consist entirely of Nova Scotia Museum Event listings and links to content on the Nova Scotia Museum websites, http://museum.gov.ns.ca. Find us on Facebook link on the NSM parent website allows Internet visitors to view Facebook postings. Decision to launch and maintain a Twitter site, titled "Nova Scotia Museum" and registered as http://twitter.com/NS_Museum. Contents on page consist entirely of Nova Scotia Museum Event listings and links to content on the Nova Scotia Museum websites, http://museum.gov.ns.ca. Follow us on Twitter link on the NSM parent website allows Internet visitors to	**3. <u>Facebook/Twitter.</u>** Not applicable	Canada. **3. <u>Facebook/Twitter.</u>** In keeping with Direction 3 of the Heritage Strategy, to increase public recognition of the value and relevance of the province's rich heritage, the Promotions team has developed a marketing plan that includes developing a dynamic online presence; a key competent of this plan is utilizing social media platforms to increase public recognition.

	view the Twitter feed without an account. Internet visitors can also view the NSM Twitter feed without a Twitter account using RSS. **4. <u>Google Analytics</u>.** novascotia.com uses Google Analytics as a website statistics software program. Google Analytics tracks website visitors via IP address and stores this information on servers located outside of Canada. The Tourism Division uses Google Analytics because of its unique ability to closely track our online tourism campaigns, goals and conversions. **5. <u>Social Media Campaign.</u>** As part of the Tourism Division's Social Media Campaign, we have posted photos, taken within Nova Scotia, by our in-house photographer Wally Hayes, on flickr, Facebook and Google Earth. Each of these companies (flickr, Facebook, and Google) are US companies and have their servers located outside of Canada. We	**4. <u>Google Analytics</u>.** All the above mentioned information is stored as part of the regular accounts being set up with Google Analytics, Google Earth, flickr, Facebook, YouTube and TripFilms. We are not able to place any restrictions or conditions on the storage or access to this information outside of the company's regular privacy standards/set-ups. **5. <u>Social Media Campaign.</u>** N/A	**4. <u>Google Analytics</u>.** Google Analytics - Individual IP addresses can not be tracked back to an individual or location without the aid of the Internet Service Provider. This information is not released by an Internet Service Provider, except under extreme circumstance such as a court order. Therefore, it was decided that using Google Analytics is acceptable. **5. <u>Social Media Campaign.</u>** The photos which are housed on servers outside of Canada (flickr, Google Earth, Facebook) are the same photos which are displayed to world on the provincial tourism website www.novascotia.com and can be easily removed at any time upon request. The videos stored on YouTube and TripFilms which feature personal information are negotiated with actors/video submitters prior to being posted on the internet and can also be

	decided to post photos and information on flickr, Facebook, and Google Earth as they are among the top performing social media websites in relation to our tourism target market. Also, as part of the Tourism Division's Social Media Campaign, we have posted videos on YouTube and TripFilms. Two types of videos have been posted. The first is Nova Scotia Tourism produced videos which have actor rights negotiated and the second are user generated videos. The creators of the user generated videos have signed Terms and Conditions which state that Nova Scotia Tourism can use their video to promote the province.		easily removed upon request.

Transportation and Infrastructure Renewal	**1. <u>Travel.</u>** Highway Engineering Services had seven (7) employees who traveled to the US. While away, these staff had the ability to access personal information carried on e-mail/stored in GroupWise. **<u>2. Travel.</u>** Highway Operations had fifteen (15) employees who traveled to the US. While away, these staff had the ability to access personal information carried on e-mail/stored in GroupWise via remote access to the GroupWise system. **<u>3. Motorola</u>** gathers and stores personal information in connection with its service obligations to Bell and the Province. The personal information they collect are the names and business telephone numbers of Bell and Province of Nova Scotia employees who have oversight duties in connection with Motorola maintenance obligations.	**<u>For # 1 and # 2 Travel</u>**. Access to the GroupWise system was protected by username/password authentication and is delivered over SLL encrypted link. **<u>3. Motorola.</u>** N/A	**<u>For # 1 and # 2 Travel</u>**. When staff travel outside Canada, they monitor e-mail to fulfill their job requirements. **<u>3. Motorola</u>.** The Act specifically excludes from its application "Material that is a matter of public record" and that names, business titles and business numbers or other like information is typically considered "material that is a matter of public record".
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	This information is subject to the Google Privacy Policy. (The Google Privacy Policy outlines its responsibility to protect any personal information it collects	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

	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 servers in the US.	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.) Equipment was password protected and accessed only by Communications Nova Scotia employees.	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. Laptops and Blackberries were necessary for presentations and to access e-mail for work.
Film Nova Scotia	Approximately three staff members traveled outside Canada on business. These staff members had the ability to access personal information carried on email or stored in GroupWise via remote access to the GroupWise email system.	N/A	When staff travel outside of Canada for business reasons, they are expected to monitor their email in order to fulfill their job responsibilities.
Atlantic Lotto Corporation	The ticketing system used by Ticket Atlantic is hosted in Irvine California, USA by Paciolan. The data is housed in their managed facility on their AS6000 mainframe computers. Secure access is provided from TCL facilities to the data centre via a secured VPN tunnel. This is data required for the sale and purchase of event tickets from Ticket Atlantic Box Office	Only Ticket Atlantic employees and agents can access the information through the secured VPN tunnel. Our contract states that Paciolan will only use the collected customer information "solely for the purposes contemplated in this agreement and otherwise in compliance with all applicable federal and state laws. The Customer will	In 2004, a tendering process was undertaken to purchase a new ticketing system. Paciolan was chosen as the bid winner as they could offer the best solution for our requirements. No vendor based in Canada could provide the same level of service necessary for our business. The software vendor only offers a hosted business model – the system is not available to be installed on premises.

	and is under the ownership of TCL.	own all Personal Information, data and related information collected or received through use of the System by it, or directly by Paciolan, and all compilations thereof, in connection with the operation of the system. Data is stored to ensure we can reconcile delivery of tickets, returns, discrepancies and payment verification to the customer. Customers are asked if they wish to receive future information on events etc., and only then will they be sent any correspondence outside the ticket purchase for which the information was supplied. Other accounts are set up by the customer to purchase tickets online and are maintained for the customer so he/she can purchase tickets online by signing into his/her TA account.	We are in our final year of the original five-year contract and have renewed for two more years. Legal council was sought on the original agreement and on the renewal in regards to best practices and privacy requirements and the contract was found to be sound.
Nova Scotia Liquor Corporation	**1. <u>Storage</u>.** There is no storage of personal information outside Canada by Nova Scotia Liquor Corporation. **2. <u>Travel.</u>** There was access to	**2. <u>Travel.</u>** The conditions placed	**2. <u>Travel.</u>** Such access is granted to

	personal information using wireless data devices including Blackberrys and laptops on a daily basis while employees were working outside of Canada.	on such access involved the use of encryption and password protection.	allow employees to perform some of their duties while absent from their offices.
InNOVA Corp	Of the 19 who traveled, 10 had access to VPM and Blackberry; 2 had access to VPN, Blackberry and Internet; 6 had access to VPN and Webmail; 2 had Blackberry access; and 7 had access to web based programs.	For business use and continuity only.	For business maintenance and continuity.
Utility and Review Board	Payroll continues to be done by Ceridian Canada who has a parent company in the US. Payroll related data may travel through or be stored on equipment accessible by the US parent.	In as much as it is possible to do Ceridian is to retain Board payroll on Canadian data sites.	No other suitable payroll service provider whose equipment is solely within Canada and without a foreign parent company has been found.
Workers' Compensation Board	Twenty-seven instances of travel with Blackberry only – access to personal information through a secure portal into the WCB's internal network. Five instances of travel with Blackberry and Laptop – access to personal information through a secure portal into the WCB's internal network.	Immediate report of theft/loss of information.	Out of country travel request to be prepared by staff and management, approved by CEO/Vice President prior to travel. The CEO/Vice President may provide direction on any appropriate restrictions to ensure we are protecting the personally identifying information to our customers.

	Six instances of travel with laptop only – access to personal information through a secure portal into the WCB's internal network.		
Nova Scotia Business Inc.	**1. salesforce.com inc.,** CRM data services/storage and access business contact information. Pursuant to s. 5(2) PIIDPA, the head of Nova Scotia Business Inc (NSBI) determined the storage/access outside Canada of business contact information in NSBIs custody/control, as part of customer relationship management (CRM) data services supplied under contract by salesforce.com inc (a Delaware, US corporation with its principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation. **2. International In-market consultants** - trade development & investment attraction services	**1. salesforce.com inc**., CRM data services/storage and access business contact information. The business contact information is to be protected in accordance with the 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 Harbour under the EU Directive on Data Privacy and is certified TRUST privacy compliant. **2. International In-market consultants** - trade development and investment attraction	**1. salesforce.com inc.,** CRM data services " storage and access" business contact information NSBI requires a robust and secure CRM platform to store and manage information necessary for the conduct of NSBIs 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. **2. International In-market consultants** "trade development &

	"storage and access" personal information (primarily business contact information) Pursuant to s. 5(2) PIIDPA the head of NSBI determined the storage / access outside Canada of personal information (primarily business contact information) in NSBIs 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 NSBI operation.	services "storage and access" personal information (primarily business contact information). The personal information (primarily business contact information) is to be protected in accordance with the service agreement including confidentiality provisions.	investment attraction services "storage and access" personal information (primarily business contact information) NSBI engages international in-market consultants as an essential and integral component of NSBIs 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 business contact information) outside Canada in order to facilitate business connections/ transactions in performing their contracted services.
	3. <u>Travel.</u> NSBI directors, officers, employees performance of duties during international travel "storage and access"personal information. Pursuant to s. 5(2) PIIDPA the head of NSBI determined the storage/ access outside Canada of personal information in NSBI custody/ control, stored in, or accessed using, a mobile electronic device by an NSBI director, officer or	**3. <u>Travel.</u>** NSBI directors, officers, employees' performance of duties during international travel "storage and access" personal information. 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	**3. <u>Travel.</u>** NSBI directors, officers, employees' performance of duties during international travel "storage and access" personal information. 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

	employee for business continuity purposes during international travel is to meet the necessary requirements of NSBIs operation.	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 and the NSBI Privacy Policy.	the person can perform work responsibilities while traveling outside Canada.

Table 2: Summary of January 1, 2009 – December 31, 2009 Foreign Access and Storage by Health Authorities

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Annapolis Valley District Health Authority (AVDHA)	**1. <u>Storage</u>.** AVHDA reviewed service provider contracts signed during the period to identify if any contracts allowed storage or access of personal information outside of Canada. No contracts were identified during this period. **2. <u>Travel.</u>** It is our estimation that approximately 30 employees traveled outside of Canada for business and may have accessed personal information via laptop, blackberry flashdrive or PDA's. **<u>Note</u>**: this does not reference physicians who have AVDHA privileges.	**2. <u>Travel.</u>** AVDHA has implemented encryption and passwords for all laptops, PDA's and Blackberry devices. Flashdrives are also encrypted. E-courier software is used to send personal information via email outside of the N. S. Health network. This ensures security of information via encryption. Employees are required to follow PIIDPA Regulations. A PIIDPA clause is included in all contracts signed at AVDHA.	**2. <u>Travel.</u>** Current storage and access to personal information outside Canada is linked to existing programs, services and software utilized at AVDHA are deemed necessary for management and operations. New programs, services and software are reviewed by the Department Head with the Privacy Officer. A Privacy Impact Assessment is conducted if deemed necessary. Guidelines have been established and formal policies and procedures have been drafted.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Capital District Health Authority (CDHA)	**1. <u>Travel</u>.** Approximately 7 employees traveled outside of Canada and may have accessed personal information via remote e-mail or Blackberry. **2. <u>Contracts</u>.** CDHA entered into 28 application maintenance contracts with the following 15 vendors: Toshiba Canada for Diagnostic Imaging; Philips Medical for Echo Cardiography; Fresenius Medical for Renal Dialysis; GE Healthcare for Diagnostic Imaging, EKG, and Cancer Centre; Varian Medical for Radiation therapy Cancer Centre; Dictaphone Solutions/Nuance for dictation system; Philips Healthcare for Respiratory/Neuro, Diagnostic Imaging, Perioerative Services; Philips Medical for Diagnostic Imaging, Quality America for Laboratory Q-Pulse software; Siemens Canada Ltd. for Diagnostic Imaging & Laboratory; Radiometer Canada for Laboratory; 3M Canada for Health Records & Rehab; Ventana, Beckman Coulter, Biomerieux, & Ortho Clinical	**2. <u>Contracts</u>.** All new and renewed contracts will have inclusion clause added to contracts requiring vendors to comply with PIIDPA legislation	**2. <u>Contracts</u>.** Current access to and storage of information outside of Canada is linked to pre-existing programs and/or systems utilized in the CDHA and deemed necessary for ongoing operations.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	Diagnostics for Laboratory systems.		
Cape Breton District Health Authority (CBDHA)	**1. <u>Travel</u>.** Approximately 4 employees traveled outside of Canada and may have accessed personal information via remote e-mail or Blackberry. **2. <u>Contracts</u>.** CBDHA entered into 16 maintenance contracts with the following venders: 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. Healthcare 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	**2. <u>Contracts</u>.** CBDHA All new and renewed contracts will have inclusion clauses added to contracts requiring vendors to comply with PIIDPA legislation.	**2. <u>Contracts</u>.** CBDHA Current access to and storage of information outside of Canada is linked to pre-existing programs and/or systems utilized in the CBDHA and deemed necessary for ongoing operations.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	Diagnostics for Vitros Analyzers.		
Colchester East Hants Health Authority (CEHHA)	Seven employees traveled outside of Canada and may have accessed personal information via remote e-mail or Blackberries.	All devices are password protected.	Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized in the CEHHA and are deemed necessary in the ongoing operations of these systems and programs.
Cumberland Health Authority (CHA)	Decisions were made to provide the following (including, but not limited to): - VPN access to Dictaphone System from Florida, US offices for remote vendor application support. - Encrypted (SSL) staff access to CHA web mail system from US locations. - Storage of information on whole disk encrypted DHA owned laptops. - Access to email using Blackberry mobile devices. Decisions regarding storage/access of	Access to information stored on CHA networks and servers is only permitted through encrypted VPN connections. All external email access is encrypted through SSL, VPN (IPSEC) or the Blackberry service. The CHA has adopted a standard of encrypting all information on laptops and media that is released outside the CHA. This includes removable media such as encrypted USB storage devices and CD/DVC's. Blackberry devices have been secured with passwords	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)
	personal information outside of Canada are pending upon further guidance, regulations, policies and procedures.	and auto-wipe features. 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 Committees. Privacy Impact Analysis must be completed on all new systems. Guidelines will be developed related to access and storage of personal information outside of Canada once the regulations are released by the Department of Justice.	
Guysborough Antigonish Strait Health Authority (GASHA)	There have been less than two decisions 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. These personnel may or may not have	Access to information 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	New systems that manage or contain personal identifiable information must undergo a Privacy Impact Analysis. Limitations are placed on vendors who may require access for maintenance procedures as 24/7 access to personal identifiable information is never permitted. No new systems containing

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	accessed personal information while outside Canada.	required to follow GASHA's privacy policies and procedures. There were no vendors who accessed personal or patient information for conditional purposes during the calendar year.	personal or private information were purchased other than SAP which was a provincial acquisition.
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 follow 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.
South Shore Health Authority (SSHA)	**1. Contracts.** South Shore Health entered into 21 contracts. None of these contracts require access or storage of personal information from outside Canada. SSHA has an agreement with manufacturer Phillips	**1. Contracts.** The following clause appears in all Requests for Proposals and Tenders awarded by SSHA: "Vendor acknowledges that in the performance of any	**1. Contracts.** Current storage and access to information from outside Canada is linked to preexisting programs/software used within SSHA and is deemed necessary for continued operations. Specific criteria for

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	Respironics for two Sleepware Systems, which allows access to our computer network from the company service helpline located in the US. **2. <u>Travel.</u>** There were three out of country business trips approved during this period. These staff may have (or had the ability to) access personal information via remote email, Blackberry, personal computer or	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 awarded Contract".	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)
	other means. Staff traveling outside the country for pleasure are asked to refrain from the use of SSHA owned devices that contain personal information. No approvals were given for staff traveling outside the country for pleasure to access information from outside the country using webmail or VPN.		
South West Nova District Health Authority (SWNDHA)	**1. <u>Travel</u>.** Ten employees were involved in international travel where they may have maintained access to the organization through cell, blackberries and/or laptops. There may or may not be others who traveled outside the country and used SWH electronic equipment for operational reasons. **2. <u>Storage and Access</u>.** For operational reasons, SWH continues to store and control access of information in the areas of Diagnostic Imaging (MRI; Nuclear Medicine Mammography). Access is de-identified whenever possible. The dictation system "Nuance" is also	**2. <u>Storage and Access</u>.** The district continues to add the inclusion clause re the management of the information in all requests for proposals and renewed or new contracts.	**2. <u>Storage and Access</u>.** SWH uses software vendors located outside Canada who maintain system remotely; for example, Meditech (health information); SAP (financial and personnel); Nuance (Transcription/dictation); Siemens (DI equipment). Again, the access to

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	managed by our district, however, VPN access is available to vendors. SWH implemented SAP in April, 2009. This provincial program did undergo a Privacy Impact Assessment.	SWH continues to review web based programs and in 2009, the district blocked access to SKYPE.	systems are managed by written agreements and monitored by SWH. Specialized lab testing unavailable in Canada or cost prohibitively in Canada are sent outside the country. SWH has implemented PIA (Privacy Impact Assessment) completion on new service acquisitions that require transmission of or access to personal information outside the country.
IWK Health Centre	**1. <u>Travel</u>.** Our records indicate 112 individuals (employees and physicians) made 152 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 systems containing personal information is possible. All information accessible remotely is encrypted.	**1. <u>Travel</u>.** 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 provincial 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	

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		devices. When connecting to the IWK Communication system messages are encrypted while on route. Passwords are mandatory (enforced through network) on all wireless handheld devices.	
	2. <u>Contracts</u> which provide for access/storage outside of Canada were reviewed for mitigation of access. If it was deemed that this access/storage was necessary, a confidentiality clause, secure network access and accountability were included in the contract and/or processes wherever appropriate.	**2a. <u>Contracts.</u>** Storage and access to 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. **2 b.** Access to Survey Monkey, a web-based surveying tool is restricted on the Health Centre network due to its server and the data	**2. <u>Contracts</u>**. The IWK has permitted access or storage of personal information outside of Canada in the following circumstances: a. 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 our health information system; BirthNet/Spacelabs in Seattle, Washington which maintains our Fetal Archiving System; GE/Deio Anaesthesia Information System, Massachusetts; and Poison Information

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		being housed outside Canada. This restriction and the rationale was implemented and communicated to IWK staff and physicians on May 1, 2009. Authorization from the head of the public body in required in order to access this tool on the network.	VDL software, California). Access to the systems is set out in written agreements and monitored by the IWK. b. In circumstances where specialized laboratory testing is not available or cost prohibitive in Canada, test resulting is done outside of Canada. When circumstances allow consent is obtained. Laboratory services tracks external referral lab tests. c. When the research sponsor is located outside of Canada, no personal identifiers are provided unless consent from the patient/legal guardian has been obtained. d. 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 US based company. The PIA is reviewed by the Privacy Manager to ensure risks around disclosure of personal information are addressed.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
			e. Certain ongoing programs which depend on treatment/patient care plans from US 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, 2009 - December 31, 2009 Foreign Access and Storage by Universities

Universities	A (Description)	B (Conditions)	C (Reasons)
Acadia University	Acadia University has no violations of PIIDPA to report this year.	Acadia University has no violations of PIIDPA to report this year.	Acadia University has no violations of PIIDPA to report this year.
Dalhousie University	**1. Financial Services**. Service provider for the creation of templates for various electronic financial services, e.g. purchase orders, bills, cheques, etc. **2. University ID Card.** Management of access and financial processes used through the	**1. Financial Services**. Limited access: only where required for maintenance and troubleshooting. Personal information stored internally. 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. **2. University ID Card**. Limited access: only where required for maintenance	**1. Financial Services**. 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 Resources departments. This service provider has been used since 2003 and offers a 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. **2. University ID Card**. This system is proprietary in nature and is only sold and supported by this company. The University's identification card is used by all staff, faculty and students for a variety

	University ID Card. **3. <u>Employment Tool</u>.** Comprehensive online tool to assist students in seeking employment.	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. The company has a support technician located in Canada who provides support whenever possible. **3. <u>Employment Tool</u>.** 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	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. **3. <u>Employment Tool</u>.** 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 identified as superior in this aspect and no similar Canadian product was identified which provides the necessary functionality and range of services.

	4. Network and Systems Upgrade. Consulting services related to the University's ongoing upgrade of its internal network and systems. **5. Wireless Products.** Service provider for wireless products for employees, long distance and teleconferencing services.	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. **4. Network and Systems Upgrade.** 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. **5. Wireless Products.** Contractual security measures: restrictions on access to and disclosure of information by service	**4. Network and Systems Upgrade.** The consultant services are provided by the current provider of the systems are being upgraded and thus has the expertise to provide the services required. These systems are necessary for the operation of integral Dalhousie computing services. **5. Wireless Products.** Mobile communications solution for employees, as well as long distance calling and teleconferencing, are essential for administrative operations of the University. Significant price advantage with this service provider through the MASH sector rates negotiated by the Province.

	6. <u>Warranty Maintenance</u>. Product warranty maintenance for electronics (Storage in United States). **7. <u>Maintenance support</u>** for product which allows University staff and faculty to <u>schedule and manage meetings</u> and	provider and their employees. Internal security measures: process in place to minimize disclosure of personal information. **6. <u>Warranty Maintenance</u>.** Personal information provided is limited to what is necessary for warranty coverage; where possible and applicable, personal information will be removed from products sent to service provider for maintenance or replacement. In many cases, the customer has already provided their personal information to service provider for warranty purposes. Customers are informed at time of collection that the information they provide will be sent to service provider outside of Canada. **7. <u>Maintenance Support</u>**. Contractual security	**6. <u>Warranty Maintenance</u>.** Necessary for Dalhousie's program as a supplier of the service provider's products. Since the service provider is the exclusive supplier of maintenance under warranty, there is no Canadian alternative available. **7. <u>Maintenance Support</u>** The ability to effectively schedule and manage meetings and activities is necessary for Dalhousie operations. This product offers superior functionality and range of service not identified in any Canadian alternatives; access rarely required.

	activities in an integrated environment.(Remote access for maintenance from United States) **8. <u>Maintenance support</u>** for academic product used extensively by faculty for <u>online teaching</u>. (Remote access from US). **9. <u>Maintenance support</u>** for statistical software product, used in course <u>teaching and research</u> (Remote access from US).	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. **8. <u>Maintenance Support</u>** 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. **9. <u>Maintenance Support</u>** Contractual security measures: restrictions on access to and disclosure of information by service provider and employees;	**8. <u>Maintenance Support</u>**. The provision of online teaching opportunities is necessary to Dalhousie academic operations. This product offers a superior range of service and functionality; and has been an established service at Dalhousie for several years, therefore would require a heavy cost to convert; access rarely required. **9. <u>Maintenance Support.</u>** Necessary for Dalhousie academic and research operations in several departments. This product offers superior functionality and range of service, according to evaluations conducted by users; access rarely required.

	10. <u>Academic software</u>: supports teaching activities and allows for online collaboration, e.g. voice, video, application sharing, etc. (Information stored on server located in Canada, however access from the US may still be required for maintenance purposes). The product is a set of applications used for	remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses. Access to personal information for maintenance purposes will rarely, if ever, be required: research using this product will rarely ever contain personal information, and dummy data can be created to illustrate a problem for maintenance purposes. **10. <u>Academic Software</u>**. The company agreed to move storage of our personal information to a server in Canada in 2008. Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees. Personal information is stored on a server located in Canada, hosted by a trusted	**10. <u>Academic Software.</u>** Necessary for Dalhousie's academic programs in a variety of disciplines; no Canadian product offers a comparable suite of products, service and functionality, combined with integration of other University computing services. Investigations found that this is the only suite of these products on the market, in Canada or elsewhere, that provide access control and integration with our existing applications. These tools are necessary for the operation of the University's academic programs, as student demand for collaborative teaching tools continues to grow.

	collaboration in teaching, which are fully integrated with other existing University applications. (Access from the United States). **11. <u>Service provider maintenance</u>** for its hardware and software products used extensively throughout the University. Mostly done on-site, however in some cases failed equipment which may contain personal information may need to be returned to service provider in the United States. **12. <u>Maintenance support</u>** for a web-based database that manages information and processes related to	service provider with whom we have existing agreements, who are also under obligations of confidentiality. Contractual measures in place to restrict access to and disclosure of information by service provider and their employees. **11. <u>Service provider maintenance</u>**. Contractual measures in place to restrict access and disclosure of personal information to service provider and its employees: access to university systems will be subject to Dalhousie protocols including time restrictions, on-site security, and audit function. Where possible, personal information will be removed from products which require service. **12. <u>Maintenance support.</u>** Contractual security measures: restrictions on	**11. <u>Service provider maintenance</u>**. Hardware and software from this service provider are used around the clock in University data centres and other operations, e.g. servers, switches, printers, etc. Maintenance coverage is necessary to our ability to maintain 24/7 operational requirements for these products. **12. <u>Maintenance support.</u>** Effectively managing information and processes for student work placements is necessary for the operation of Dalhousie co-operative education programs, particularly in Architecture, Commerce, Computer Science, and Engineering. Cost prohibitive for Canadian alternative; access rarely required.

	student work experience placements in industry. (Remote access from US). **12. Maintenance support** for product which allows for real-time synchronization of faculty and staff calendars with wireless tools. (Remote access from US). **13. Plagiarism Detection**. Academic program: online plagiarism detection service (Storage in US).	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. **12. Maintenance support.** 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. **13. Plagiarism Detection.** Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; Storage of Dalhousie information will	**12. Maintenance support**. Making calendars available on the wireless tools used by the faculty and staff who are required to use them is necessary for Dalhousie operations. There is no suitable Canadian alternative, given Dalhousie IT architecture and costs to convert; access rarely required. **13. Plagiarism Detection**. Necessary for Dalhousie's academic programs in order to maintain high standards of academic integrity. There is currently no product in Canada offering a comparable range of service and functionality. Minimal personal information disclosed.

	14. <u>Maintenance support</u> for product which supports all major University <u>administrative computing applications.</u>(Remote access from US or Bangalore, India) **15. <u>Maintenance support</u>** for product which allows University staff and faculty to <u>schedule and manage meetings</u> and activities in an integrated environment. (Remote access from US).	be segregated from other users; Internal security measures: process in place to minimize disclosure of personal information. **14. <u>Maintenance support.</u>** 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. **15. <u>Maintenance support</u>**. 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.	**14. <u>Maintenance support</u>**. Necessary service for the operation of integral Dalhousie academic computing services; no Canadian alternative identified; access rarely required. **15. <u>Maintenance support</u>**. The ability to effectively schedule and manage meetings and activities is necessary for Dalhousie operations. This product offers superior functionality and range of service not identified in any Canadian alternatives; access rarely required. **16. <u>Maintenance support</u>**. The ability to effectively manage room bookings across campus

	16. <u>Maintenance support</u> for facilities management product used for <u>reserving rooms on campus</u>, specifically for event and classroom scheduling.(Remote access from US). **17. <u>Maintenance support</u>** for academic product which provides students with <u>information regarding their progress</u> towards meeting their degree requirements (Remote access from US). **18. <u>Maintenance support</u>** for a scheduling and data	**16. <u>Maintenance support.</u>** 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. **17. <u>Maintenance support.</u>** 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. **18. <u>Maintenance support.</u>** Contractual security measures: restrictions on	through one centralized program is necessary for Dalhousie operations. This product offers superior functionality to the identified Canadian alternative, and there would be a heavy cost to convert in terms of labor and acquisition costs. Access rarely required. **17. <u>Maintenance support</u>**. Allowing students to access their information regarding progress towards degree requirements is necessary for Dalhousie operations, particularly in student advising and counseling, and for the Registrar's Office. No Canadian alternatives have been identified; access rarely required. **18. <u>Maintenance support</u>**. Providing advising and counseling services to students, and effectively managing and tracking those services, is necessary for Dalhousie student services operations. This product offers superior functionality and range of service; access rarely required.

	tracking software, designed for university student advising and counseling (Remote access from US). **19. Maintenance support**. Maintenance support for student services product which allows faculty members to convey concerns to students about aspects of class performance and provide referral to on-campus resources.(Remote access from US). **20. Evaluations**. Software product used to collect and maintain evaluations specifically in the medical education field (e.g.	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. **19. Maintenance support**. 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. **20. Evaluations**. Data is stored internally. Contractual security measures: restrictions on access to and disclosure of information by service provider and	**19. Maintenance support**. The ability to identify and address potential student performance issues at the earliest possible stage is necessary for the Dalhousie operations in terms of enhancing the student experience. No Canadian alternatives identified; access rarely required. **20. Evaluations**. Medical education evaluations are a necessary requirement of the operation of our Faculty of Medicine; proper management of these evaluations is critical to decision-making with respect to promotion throughout a student's medical education. This tool was originally investigated and purchased when it was 100% Canadian-owned and operated, and a determination was made at that time that it was the most effective tool for our purposes.

	student evaluations, preceptor evaluations, etc.). This product was originally developed in Canada, however is now a wholly-owned subsidiary of a US company. Product is still maintained in Canada.	employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, pre-approved IP addresses, and segregation of personal information where possible. Vendor agrees that any remote access will only occur from within Canada.	
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, S. C., 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. When they travel, Kings employees may take personal information out of the country temporarily on laptop computers and electronic devices such as Blackberries and cell phones. They are also permitted to remotely access personal information while	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.

		traveling abroad. Transporting and remote accessing of personal information in this fashion, however, is only permitted when necessary for the performance of the employee's duties. Employees must take reasonable precautions to protect the information. For instance, laptops should be secured against theft when traveling and employees should avoid submitting marks or accessing students' personal information online while outside the country. Personal information may be disclosed outside Canada when the person involved has consented to disclosure or when disclosure is required under Canadian law or a treaty. Personal information may also be disclosed outside Canada 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 must notify the Minister of Justice immediately if a foreign court, law enforcement agency or other authority demands disclosure of personal information under its control. 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.	

St Francis Xavier	**1. The University's financial software "Bi-Tech"** is provided by an American software vendor Sungard Bi-Tech (since 1988). This software requires periodic maintenance and updates. These maintenance needs and updates are applied to our financial software through a remote access link between our server and a "Bitech" 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. **2. Kinetics Software** (Kx) is a comprehensive software program that	1. The university has taken steps to minimize our exposure to risk by restricting access to our system to designated and prescheduled time periods and only when maintenance and update activities cannot be accomplished by university personnel. We are working with a mature software product and, historically, access has been for semi-annual updates only, therefore, we have minimal exposure points. 2. Vendor provides technical support, through remote access, previously arranged with the university	1. The cost of switching our software vendors is cost prohibitive at this time. 2. The only method of receiving technical support is through remote access by the vendor.

	manages catering, facility and residential bookings. It is comparable to large conferencing or hotel management systems. The Conferences and Special Events Department at the university uses this program as our main software to support our operations, making use of the Events, Residential, Catering, Marketing and Extracts modules available within the software. **<u>3. Course on-line management system.</u>** System stores names, student ID numbers and meal plan details. Storage is on server in Canada onsite. Remote access is only permitted when a technical issue arises that cannot be resolved	technology support group for each incident. 3. Vendor provides technical support through remote means previously arranged with the university's technology support group for each incident.	3. The only method of receiving technical support is through remote access by the vendor.

	by other means.		
Nova Scotia Community College	**<u>1. Storage.</u>** The Nova Scotia Community College has allowed for the storage of personal information under its control to be held by Hobsons EMT (formerly Apply Yourself, Inc.). This company is located in Fairfax, Virginia (USA). Hobsons EMT is an application service provider offering web-based data management for the College's online application process. **<u>2. Travel.</u>** The College will allow our employees to transport personal information temporarily outside Canada.	1. The services of Hobsons EMT are required to support the application process for many of our student applicants. The College will provide notification to electronic applicants indicating that Hobsons EMT is an American company and the access and use of applications is subject to all applicable federal, state and local laws. 2. The personal information transported outside Canada has to be strictly necessary for their assigned duties or as a necessary part of a research project. The	1. The College has been using the services of Hobsons EMT effective March 21st, 2005, prior to the Assent of the Act on July 14th, 2006. Since our last submission (March 24th, 2009), we have not actively investigated service providers within Canada, however, there have been no emerging or known Canadian companies identified by us 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 our current database service provider (Oracle/PeopleSoft) and products. Currently, none are ready for implementation, however, it is our understanding a solution is under development and may be ready to purchase in 2010. In September, 2009, the College began a project to investigate possible strategies and solutions with the aim of replacing Hobsons EMT in the later part of 2010.

	3. Accessing personal information in College data repositories from outside Canada.	transport is anticipated to be through use of cellular telephones, wireless handhelds, laptops and storage devices. In such event, employees will be required to take all reasonable precautions (e.g., encryption) to protect the personal information. 3. 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.	
Université Sainte-Anne	The only instances where personal information under the custody of the Université was accessed outside of Canada would be when employees access their e-mail accounts over the internet on their Blackberry or	The restrictions or conditions placed on storage or access of the personal information outside Canada was limited to password protection to e-mail accounts.	As certain key employees are from time to time out of the country for extended periods of time, it has been deemed necessary to allow them access to these e-mail accounts in order to perform the duties assigned to them by the Université.

	telephone.		
Cape Breton University	**1. <u>Alumni/Donor Database</u>.** 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	**1. <u>Alumni/Donor Database</u>.** Access to systems is restricted to authorized personnel only - ¾ access occurs only for the purpose of receiving technical support that cannot be accomplished internally. Access to information is authorized for the purpose of required assigned duties and research.	**1. <u>Alumni/Donor Database</u>.** The University's demand for requesting technical support is minimal to nonexistent 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. Storage and access, as required, to meet the operational requirements of the University.

	access. This access is restricted to the screen view only and controlled by the database administrator. Once the support is concluded, access is automatically terminated. **2. <u>Travel</u>.** Approximately 65 staff members traveled outside of Canada and may have (or had the ability to) access personal information via remote email, Blackberry, personal computer or by any other means. While traveling outside the country, such access is necessary for university administrators, researchers and other employees to perform their assigned duties or as a necessary part of a research project.		

Nova Scotia Agricultural College	**1. <u>Student Information System</u>.** The NSAC allows our Student Information System (SIS) provider, Datatel Inc., to provide tier II application maintenance/support to our 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 Office, Residence Services). The system houses all academic and student financial account information, as well as alumni and	**1. <u>Student Information System</u>.** Administrative rights are controlled by the NSAC Database Systems Administrator with username/password authentication for TCP/IP connectivity being granted to Datatel as required. As noted above, 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. As well, 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.	**1. <u>Student Information System</u>.** When the 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 of 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 our daily business the NSAC must continue to have Tier II support provided by this vendor.

	campaign information. The SIS is a mission critical system that supports the core business activities of the NSAC. Datatel is one of the leading North American SIS providers, with their head office located in Fairfax, Virginia (http://datatel.com). Datatel accesses our system on a monthly basis to solve problems that are not resolved by our first level of support which is provided by our in-house Database Systems Administrators. All access is via TCP/IP protocol. NSAC stakeholder access is restricted to internal NSAC network 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 Corporate Services Unit - IT Division.		
Nova Scotia College of Arts and Design (NSCAD)	Move from various systems including to a single unified Enterprise Resource Planning (ERP) system provided by Datatel Inc. of Fairfax, VA.	Access to personal information is to be limited to Datatel personnel providing support for the ERP system using remote access technology in case of issues with the system. All data will remain resident on NSCAD servers located in Nova Scotia.	All major academic ERP vendors (Datatel, Sungard and PeopleSoft) are based in the United States. To design and implement a home-grown ERP system would be cost-prohibitive for an institution NSCAD's size.

Table 4: Summary of January 1, 2009 - December 31, 2009 Foreign Access and Storage by School Boards

School Boards	A (Decision)	B (Conditions)	C (Reasons)
Strait Regional School Board	**1. <u>On-line Subscriptions</u>.** The Strait Regional School Board currently holds on-line subscriptions for Discovery Education (formerly Streaming and Reading A to Z). These are on-line subscriptions to education media. The teacher's name and school are provided to both on-line education media providers. This contract has been in existence prior to December 15, 2006. **2. Travel.** To our knowledge, 29 employees traveled outside of Canada and may have (or had the ability to) access personal information as outlined below: Web mail - 29 employees (Cities and Countries: Cancun, Mexico; Phoenix,	**1. <u>On-line Subscriptions</u>.** Our network allows secure VPN access only. More specific guidelines related to access and storage of personal information outside of Canada are currently being researched and developed.	**1. <u>On-line Subscriptions</u>** Functionality of the operations of the board are deemed necessary for management and operations.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	Arizona, Orlando, Florida, Caribbean, New York, Las Vegas, Nevada, Boston, Massachusettes, Punta Cana, Dominican Republic, Cambridgeshire, UK and New Hampshire) Of these 29 employees, 8 used their blackberry and five used their laptop.		
Halifax Regional School Board	Eight staff members traveled outside of Canada which would have had access to personal information via their Blackberries.	Relevant HRSB policies would apply to Blackberry usage outside of Canada. Each Blackberry is password protected. The HRSB will incorporate into its policy direction on access and storage of personal information outside of Canada.	The staff members at issue occupy management positions and must be available by e-mail for decision-making and information purposes.
Tri-County District School Board	No storage or access outside of Canada	N/A	N/A
Annapolis Valley Regional School Board	No storage or access outside of Canada	N/A	N/A

Table 5 - Summary of January 1, 2009 – December 31, 2009 Foreign Access and Storage by Municipalities[2]

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
Municipality of the District of Barrington	Municipal property owners living outside Canada are sent property tax invoices every year by the Municipality. Information related to these invoices and the related properties is regularly exchanged with the property owners.	No information is stored outside Canada by the Municipality. The only restrictions placed on the information are those required by FOIPOP legislation.	
Municipality of the District of Lunenburg	One employee traveled outside Canada and had the ability to access personal information carried on e-mail by way of Blackberry.	The Blackberry is not set up to access the Municipal server.	The employee monitors e-mail and voice mail where possible and when required.
Municipality of the County of Kings	One staff member traveled outside Canada during the reporting period and had the ability to access corporate e-mail via corporate	Remote access is protected by username/password and is delivered over an encrypted link.	The staff member in question was approved for travel by the CAO and was expected to maintain a means of communication with their respective staff in order to fulfill operational responsibilities/requirements.

[2] Municipalities of the Towns of Shelburne, Kentville, Annapolis Royal, Amherst, Antigonish, Pugwash, Lockeport, Bridgewater, Hantsport, Pictou, Parrsboro, Port Hawkesbury, Liverpool, New Glasgow, Digby, Springhill, Stewiacke, Truro, Shelburne, District of St. Mary's, Municipality of the Counties of Victoria and Annapolis and Cape Breton Regional Municipality had no access or storage outside of Canada to report. Halifax Public Libraries and Cumberland Joint Services Management Authority did not have anything to report as well as the Municipality of the District of West Hants.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	notebook computer.		
Village of Bible Hill	Chairperson took a laptop computer (owned by the Village of Bible Hill) to Florida. The purpose was to send and receive e-mails through a Village of Bible Hill e-mail account.	The computer did not have access to a Bible Hill server or other data files.	No other data access occured other than e-mail.
Municipality of Colchester	Four staff members traveled outside Canada. It is known that two staff 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. We have an approved policy that requires employees to limit any personal information being sent while visiting/working outside of Canada, and if they are taking electronic equipment, they are	When staff travel for business or personal reasons, they may be expected to monitor their business e-mail in order to fulfill their job responsibilities.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
		required to report their intention to senior management.	
Municipality of East Hants	A decision was made to purchase a Human Resource Information System (HRIS) from ADP Canada Co. Personal data of the employees of East Hants is stored in ADP Canada's database in Mississauga, Ontario, however, the server through which the data is accessed resides in New Jersey, United States.	In the terms of the contract with ADP Canada for the HRIS, the Municipality is requesting language to indicate that the Municipality is to be alerted whenever data is accessed under the Patriot Act.	Prior to the introduction of PIIDPA, the Municipality contracted ADP Canada to provide payroll services as well as support a time management application purchased through ADP Canada. The HRIS application is the umbrella software for the payroll and time management applications already being used by the Municipality and, therefore, the decision to purchase the new HRIS module was the most cost effective and prudent use of public funds.
Halifax Regional Municipality	**1. <u>Travel</u>.** Between January 1st and December 31st, 133 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.	**1. <u>Travel</u>.** Prior to traveling, staff were advised that HRM Communication tools (Cell Phones, Blackberries, laptops, memory sticks, VPM) were to be password protected.	**1. <u>Travel</u>.** 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.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	2. <u>System Support and Maintenance</u>. The following venders (Versaterm (Police RMS, CAD 911), Hansen (Tax Bill, Customer Service, Permit/License) and RIVA (PSAB Compliance-Financial) were provided access on an approved, need basis to the applicable production systems for support and maintenance.	**2. <u>System Support and Maintenance</u>.** Vender access is controlled and monitored by IT support staff.	**2. <u>System Support and Maintenance</u>.** Vendor access is necessary for the systems to continue to function properly.
Halifax Regional Water Commission	Halifax Water authorized 43 staff members to transport personal information devices such as laptop computers, cell phones and electronic data storage devices outside of Canada.	These devices were taken by staff to ensure they remained in contact with other utility staff to fulfill operational responsibilities.	Halifax Water owns and operates water, wastewater and stormwater systems which are deemed critical infrastructure by the Government of Canada.