



**Nova Scotia Personal Information International
Disclosure Protection Act**

2006 Annual Report

**NS Department of Justice
First Reporting Period**

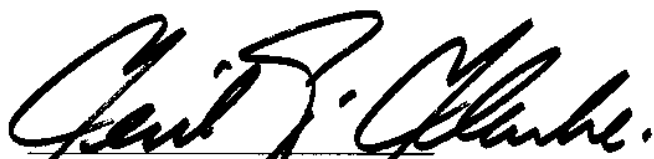
Message From The Minister Of Justice

I am pleased to provide the first 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 passed by Nova Scotia government on July 14, 2006, and became effective on November 15, 2006, for public sector entities and November 15, 2007, for municipalities.

PIIDPA was created to enhance provincial privacy protection activities, and at the same time respond to Nova Scotian concerns about the vulnerability of public sector and municipal personal information holdings to foreign access, storage and disclosure. The Act prohibits public sector entities, municipalities and their service providers from allowing foreign storage, disclosure or access to personal information, except to meet the "necessary requirements" of a public sector or municipal operations.

Under PIIDPA subsection 5(3), Nova Scotia public sector entities are required to report the decision and description of any foreign access and storage of personal information occurring between December 15 to December 31, 2006, to the Minister of Justice. This report is based on the public sector reports received by the Department of Justice, thus it is our view that the information contained in this report is generally an accurate representation of activity under the legislation.

This report contains a summary of the 24 public sector 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.



Hon. Cecil P. Clarke
Minister of Justice

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 December 15 -31, 2006 Foreign Access and Storage by Government Departments

Department	A (Description)	B (Conditions)	C (Reasons)
Education	<p>The Department utilizes Oklahoma Scoring Services (OSS) software for the purpose of storing and processing information, in support of the General Educational Development (GED, high school equivalency) program. A Virtual Privacy Network (VPN) and File Transfer Protocol (FTP) are used to send the encrypted, scanned test results to OSS. The encrypted exam results and certificates are securely transmitted back to the Department using a VPN and FTP.</p>	<p>The Department has signed a contract with OSS, which stipulates that all information will be kept private and confidential. Additionally, the contract specifies that personal information will not be released to any third party unless authorized by the Department in writing. The contract also states that only personnel authorized by the Department will be provided access to store and retrieve NS information.</p>	<p>Both suitable GEDTS certified vendors are located in the USA. OSS has extensive experience, has mature software, secure transmission methods and has a good reputation.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
Finance	Remote access via secure network connections to provide routine SAP support maintenance. SAP is an internal enterprise resource planning system used for finance, human resources and procurement. SAP support staff are located in the US, Germany, and India. However, this remote access very rarely involves access of personal information. The personal information retained in the SAP is about current and past government employees, e.g., pensioners.	Access has to be approved by the Corporate Information Services Division management and all access activity is recorded in an audit log.	There is no alternative method for providing IT support for the SAP system.
Health	Three staff members travelled outside Canada on business. These staff members had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise email system.	The Department of Health <i>Transmission of Confidential Information by E-mail and Fax Guideline (2004)</i> prohibits the inclusion of personal information contained in e-mail, unless the e-mail is encrypted and password protected.	When staff are travelling for business reasons they are expected to monitor their e-mail and voice mail where possible in order to fulfill their responsibilities.

Department	A (Description)	B (Conditions)	C (Reasons)
Health Promotion and Protection	One staff member travelled outside Canada on business. This staff member had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise e-mail system.	The Department of Health Promotion and Protection <i>Transmission of Confidential Information by E-mail and Fax Guideline (2004)</i> prohibits the inclusion of personal information contained in e-mail, unless the e-mail is encrypted and password protected.	When staff are travelling for business reasons they are expected to monitor their e-mail and voice mail where possible in order to fulfill their responsibilities.
Intergovernmental Affairs	Off site paper document storage contracted with Iron Mountain Canada (subsidiary of the American company).	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 held by Iron Mountain are to be held in confidence as per the agreement. Iron Mountain will use the same degree of care to safeguard this information as it utilizes to safeguard its own confidential information.	Due to limited storage space for business records, Intergovernmental Affairs required off site storage. At the time of the contract, 2006, there was no Canadian-owned competitor in NS and Iron Mountain is considered to be the industry lead.
Service Nova Scotia and Municipal Relations	a. The Interprovincial Record Exchange (IRE) system allows Canadian motor vehicle jurisdictions to securely query other jurisdiction's driver and vehicle records. The Canadian Council of Motor	a. CCMTA does not provide direct read access to another jurisdiction's system, but CCMTA and AAMVA pre-formatted queries CCMTA are specific to the type of information that is displayed. CCMTA has	a. Promotion of road safety and law enforcement so that a driver's license or vehicle permit may not be fraudulently transferred from one jurisdiction to another.

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>Transport Administrators (CCMTA) disseminates the IRE information, administers the system and operates the secure network. There is a partnership arrangement with the American Association of Motor Vehicle Administrators (AAMVA) to extend the IRE system to the US.</p> <p>b. Digimarc, Indiana, has a contract to provide Photo Licence/Photo ID equipment, software integration and support services to the Registry of Motor Vehicles. (This contract expires in 2008 and will be replaced with a new contract under the joint Atlantic Canada Photo Licence Project). The Photo Licence Oracle server that stores client photos, digitized signatures, personal information, and Driver Master Numbers is located at the Provincial Data Centre in Halifax. Two Digimarc support technicians were provided remote access via VPN to</p>	<p>contracts with each of its member jurisdictions that conform to the jurisdictions's privacy legislation concerning disclosure and consent.</p> <p>b. Access from Indiana is restricted via VPN username/password to these two support technicians, and on the Oracle server by a privileged account username/password. Access will be in response to escalated support calls only.</p>	<p>b. Access by Digimarc is an operational requirement in response to Photo Licence/ Photo ID outages that affect the delivery of customer service.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>provide backup maintenance and support to the local Digimarc technician, or to manage escalated problems.</p> <p>c. Nine SNSMR staff members travelled outside Canada during the reporting period and accessed GroupWise e-mail from a laptop or Blackberry™ while away.</p> <p>d. An American company, Tyler/CLT, was given controlled access to property assessment data for the purpose of converting and transferring that data from Assessment's legacy system to the new iasWorld system. Tyler/CLT continues to have controlled access to the system, which houses assessment data for the purpose of servicing and maintaining the system. All data remains in Canada, and remote access by Tyler/CLT was tightly controlled.</p>	<p>c. Remote access to GroupWise is protected by username/password authentication, and is delivered over an SSL-encrypted link.</p> <p>d. Contractor access is only allowed through a restricted and audited VPN account. Contractors can only access a terminal server, which has been configured for data conversion purposes. The terminal server is configured to not allow data transfers to other computers, i.e., files cannot be e-mailed or copied to themselves or another network. Contractor activity is reviewed and monitored via the audit logs.</p>	<p>c. To maintain contact with operations.</p> <p>d. The iasWorld system was the only Computer Aided Mass Appraisal (CAMA) system that met all the Assessment Divisions requirements. Tyler/CLT services the legacy system and produced the core CAMA component of the new iasWorld system, thus had the expertise to convert the data from the old to the new system and to service iasWorld on an ongoing basis.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
<p>Tourism, Culture and Heritage</p>	<p>a. The Department has a marketing partnership with Bay Ferries Ltd, who operate the CAT Ferry from Portland, Maine and from Bar Harbor, Maine. A part of this partnership includes exchanging leads or literature requests with Bay Ferries through the same fulfillment centre used by the Department.</p> <p>b. The Department has a contract with Cloutier Direct Inc. (CDI) of Scarborough, Maine to mail Nova Scotia tourism information to people who have requested information from the province. Requests are received through the Department's Halifax-based customer contact system, call centre, Novascotia.com web site and regular mail requests. CDI daily downloads US and International information requests to send out the requested information from the contact centre.</p>	<p>a. The leads may only be used to promote Nova Scotia or Bay Ferries as a transportation partner to Nova Scotia. The leads may only be used once and any other use must be approved by the Department.</p> <p>b. Names and addresses may only be used to fulfill requests received by the Department, who own the database. CDI may only use the names and addresses once, unless approval is provided by the Department.</p>	<p>a. Partnering with Bay Ferries and exchanging leads increases the Department's marketing reach and helps promote the various ways to get to Nova Scotia. The partnership allows leverage of financial resources to further promote Nova Scotia and grow the tourist industry.</p> <p>b. CDI was contracted to provide literature to potential visitors in a prompt and cost efficient way. The Department previously fulfilled US and International requests from Canada, but the delivery time was too long and too expensive for the service received.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
Transportation and Infrastructure Renewal	<p>a. Telecom Service Group awarded the contract to monthly re-bill government users' telecommunication services to Symphony Services, located in Dallas, Texas. Symphony Services will have access to the current Tru Server application to complete the transition to the Expense Management System (EMS). The server is located in Halifax and will be accessed remotely by Symphony Services in Dallas. Access will only be made available during scheduled times and will be monitored by Government employees.</p>	<p>a. Symphony Services will not have the ability to remove or copy files. Once the conversion is complete, access will be disabled and only re-enabled during scheduled support services work.</p> <p>Symphony Services has read, understands and has signed off on PIIDPA obligations. Government employees may travel to Symphony Services offices to inspect the security measures used to protect personal information.</p>	<p>a. The EMS application was the best fit for the Telecom Service Group operational requirements. The was not a cost-effective Canadian solution available.</p> <p>Symphony Services has supplied the previous two telecom billing services, thus are familiar with the Provincial requirements. Their experience with migrating other clients to EMS lowers the Province's risks associated with migration of data. The EMS application server will provide a stable, secure operating environment. The Department will be able to use the existing Oracle corporate licence agreement and will allow use of other current software that was not compatible with Tru Server.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>b. The Insurance and Risk Management (IRM) Group awarded the contract to supply and support the STARS software to CS STARS LLC, located in Chicago. STARS is used for claims management and insurance inventory by the Province. The data will be stored in Chicago and remotely accessed by IRM via a Halifax server.</p>	<p>b. CS STARS LLC has read, understands and has signed off on PIIDPA obligations. Government employees may travel to the CS STARS LLC offices to inspect the security measures used to protect personal information.</p>	<p>b. STARS fits the operational requirements of the IRM Group and there was no cost effective Canadian solution available. The Province has used the STARS system for 10 years.</p>
Agencies	A (Description)	B (Conditions)	C (Reasons)
<p>Utility and Review Board</p>	<p>The Board continues to use an external service provider, Ceridian Canada, to process payroll for the Board staff. The personal information is not stored outside of Canada. The parent company is American, thus Ceridian is subject to the US <i>Patriot Act</i>.</p>	<p>No disclosure of any kind to anyone other than authorized Board staff.</p>	<p>Data is not stored outside of Canada. Ceridian will be used until a suitable wholly Canadian source provider can be found.</p>

Table 2: Summary of December 15 -31, 2006 Foreign Access and Storage by Health Authorities

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Annapolis Valley District Health Authority (AVDHA)	<p>Two service provider contracts were renewed:</p> <ol style="list-style-type: none"> 1. Pinestar Technology Inc., one-year software maintenance; and 2. Carenet Services Inc., one-year Electronic purchasing. <p>It is estimated that between 15 to 20 employees travelled outside of Canada for business and may have accessed personal information via laptop, Blackberry™ or PDA's.</p>	AVDHA has started the implementation of encryption and passwords for laptops, Blackberry™ and PDA's.	Current storage and access to personal information outside Canada is linked to pre-existing programs, services and software utilized by AVDHA to ensure efficient operations.
Cape Breton District Health Authority (CBDHA)	<p>Approximately five employees travelled outside of Canada and may have accessed personal information via remote e-mail or Blackberry™. CBDHA entered into a 12-month contract for diagnostic imaging maintenance with Toshiba Canada that there may be a possibility for access outside of Canada.</p>	Awaiting PIIDPA Regulations.	Current storage and access to personal information outside Canada is linked to pre-existing programs and systems utilized by CBDHA and are deemed necessary for ongoing operations.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Capital District (CDHA)	Approximately three CDHA staff members travelled outside of Canada and may have (or had the ability to) access personal information via remote e-mail, Blackberry™, personal computer or by any other means. Note: this does not reference physicians who have CDHA privileges.	CDHA general information and sharing policies apply in this situation. More specific guidelines related to access and storage of personal information outside of Canada are under development.	Current storage and access to personal information outside Canada is linked to pre-existing programs and systems utilized by CDHA and are deemed necessary for management and operations.
Colchester East Hants (CEHHA)	Approximately three staff members traveled outside of Canada and may have accessed personal information via remote e-mail, Blackberry™ or Treo™ . No contracts were signed during this reporting period.	Guidelines will be developed relating to access/storage of personal information outside of Canada once the PIIDPA Regulations are implemented.	Access and storage of personal information outside of Canada is linked to pre-existing programs and/or systems utilized by CEHHA and are deemed necessary in the ongoing operations of these systems and programs.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Cumberland Health Authority (CHA)	VPN access to Dictaphone System, Florida, for remote vendor application support. VPN access to Saturn OR, US, for remote vendor application support. Staff access to CHA encrypted web mail system from US locations. Storage on information on whole disk encrypted laptops.	Access to information stored on CHA networks and servers is only permitted through encrypted VPN connections. All external e-mail access is encrypted through SSL or VPN. There is a standard for encrypting all information on laptops and media that is released outside the CHA, including removable devices such as USB storage devices and CD/DVD's.	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)
Guysborough Antigonish Strait Health Authority (GASHA)	<p>a. Once or twice a year GASHA staff who use a Blackberry™ (primarily senior managers) travel outside of Canada. These staff need to have access to their e-mail so they can be contacted while away from the office. Their e-mail is provided by CDHA and the NotifyLink service at the IWK Health Centre.</p> <p>b. Occasionally GASHA staff travel outside of Canada and take laptops to work on reports, etc. To access files or systems stored in the DHA, they use a VPN provided by CDHA.</p> <p>c. Staff need to have access to e-mails (as provided by CDHA) via the internet so they can be contacted while away from the office.</p>	<p>No restrictions.</p> <p>b. Not all staff have laptops and there is a policy regarding encrypting the laptops, as of March 2007 the policy was not implemented.</p> <p>c. No restrictions.</p>	<p>The senior managers with Blackberries™ need to be accessible while outside of Canada. The information they would be accessing is their own e-mail, including contacts and calendars.</p> <p>b. Taking a laptop outside of Canada is a rare practice, however with deadlines access may be needed with the staff member is outside of Canada.</p> <p>c. E-mail accessible through the internet provides timely responses that may improve the overall decision making process.</p>

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Pictou County Health Authority (PCHA)	There were no new or renewed contracts. VPN access to Dictaphone System, Florida, for remote vendor application support. VPN access to Saturn, Oregon for remote vendor application support. Staff access to PCHA encrypted web mail system from US locations. Storage on information on who disk encrypted laptops.	Access to information stored on PCHA networks and servers is only permitted through encrypted VPN connections. All external e-mail access is encrypted through SSL or VPN. There is a standard for encrypting all information on laptops and media that is released outside the PCHA, including removable devices such as USB storage devices and CD/DVD's.	Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized in the PCHA and are deemed necessary in the ongoing operations of these systems and programs.
South Shore Health Authority (SSHA)	SSHA entered into two contracts that may require access or storage outside of Canada: 1. Annual software support for software support from Hewlett Packard. 2. Electronic purchasing from Carenet Services.	Conditions or restrictions for new contracts will be developed once the PIIDPA Regulations are implemented.	Current storage and access to information outside Canada is linked to preexisting programs/software used within SSHA and is deemed necessary for continued operations.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
South West Nova District Health Authority (SWNHA)	<p>Approximately three staff members travelled outside of Canada and may have accesses personal information via remote access or Blackberry™. At the time of this reporting period, four contracts were renewed:</p> <ol style="list-style-type: none"> 1. Nova Industrial, one-year leased tank maintenance; 2. East Coast Capital, three-year IS equipment lease; 3. Pinestar Technology Inc., one-year software maintenance; and 4. Carenet Service Inc. Electronic purchasing, one-year. 	Developing an inclusion clause for contracts upcoming in 2007.	Access and storage from outside Canada is linked to pre-existing programs and/or systems utilized at the SWNHA, which are required for ongoing operations of these systems and programs.

District Health Authority	A (Decision)	B (Conditions)	C (Reasons)
IWK Health Centre	There were no new contracts involving access and storage of personal information outside of Canada.	Storage or access to personal information outside of Canada by service providers and partners is done either under contract with language addressing confidentiality or with consent of the individual.	<p>To ensure compliance with PIIDPA, the IWK surveyed and created an inventory of contracts and partnerships whereby personal information may be accessed/stored outside Canada. A review of existing agreements and practices regarding access and storage revealed:</p> <ol style="list-style-type: none"> 1. Software suppliers/ vendors who remotely maintain a system are located outside of Canada. Access and storage is linked to pre-existing programs and systems related to patient care and service delivery, which are required for continued management and operations of the health centre. 2. The offsite storage/retrieval/ shredding vendor is a subsidiary of a US based company. The information is not transferred outside of Canada. 3. Some specialized laboratory testing may not be available or is cost-prohibited in Canada, thus must be done outside of Canada. Consent is obtained when circumstances allow. 4. Where specialized program specific treatment/patient care plans are not available in Canada, consent is obtained prior to the submission of personal information. 5. When a research sponsor is located outside of Canada, no personal identifiers are provided to the sponsor. All cases are coded with a unique study number. If for some reason personal identifiers are required, consent is obtained.

Table 3: Summary of December 15 -31, 2006 Foreign Access and Storage by Universities

Universities	A (Description)	B (Conditions)	C (Reasons)
Dalhousie	University administrators, researchers and other employees e-mail, data on University information systems, and research data using web-based or other internet access tools from outside Canada, while travelling on University-related business where such access is necessary for them to perform their assigned duties or as a necessary part of a research project.	Dalhousie has implemented policy entitled the “Policy for the Protection of Personal Information from Access Outside Canada” to address the requirements of the Act.	See A and B.
University of King’s College	N/A	King’s employees travelling abroad transport and remotely access personal information as their duties require and in accordance with guidelines set by the University.	Storage and access as required to meet the operational requirements of the university.

Universities	A (Description)	B (Conditions)	C (Reasons)
St Francis Xavier	The University's financial software "Bi-Tech" is provided by an American vendor, Sungard Bi-Tech, and the Bi-tech server is located in California. The periodic maintenance and updates are done through a remote access link. The access to the University's 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.	Access to systems is restricted to designated and prescheduled time periods and only when maintenance and update activities cannot be accomplished by university personnel.	This is a mature software product and historically access has been for semi-annual updates only. The cost of switching software vendors is prohibitive at this time.

Table 4: Summary of December 15 -31, 2006 Foreign Access and Storage by School Boards

School Boards	A (Decision)	B (Conditions)	C (Reasons)
South Shore Regional School Board	Education Department coordinators and consultants have the ability to access student information while outside of Canada, as authorized by the Head of this local public body. No other cases of access or storage have been authorized.	Access to information is authorized for the purposes of student case management.	Access is required for student case management functionality purposes.
Strait Regional School Board	There are on-line subscriptions for “United Streaming” and “Reading A to Z” (education media). The teacher’s name and name of school are provided to both on-line education media providers. During a conference in Massachusetts, one employee used a Board-issued laptop and Blackberry™ to access e-mail. This was a one-time only access and no storage occurred.	The network allows secure VPN access only.	Functionality of the operations of the Board.