OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Information Sharing Agreements:

Essential Administrative Safeguards

Motor Registration Division

Service NL

August 4, 2017

Table of Contents

Executive Summary

The *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015)* authorizes audits of public bodies by the Office of the Information and Privacy Commissioner (OIPC). The OIPC's Audit and Compliance Program addresses matters such as evaluating the adequacy of public body safeguards to protect personal information and compliance with the *Act*.

Citizens expect the OIPC, as the oversight body, to:

- assess compliance with the law;
- advocate for best practice; and
- assist public bodies in establishing effective privacy management programs.

This is the second comprehensive audit completed by the OIPC.

The purpose of this Report is to document best practices in Information Sharing Agreements (ISAs), taking into consideration the public body's obligations under the *ATIPPA, 2015*. ISAs are a commonly used administrative safeguard when information is being shared between entities; they are especially important if sharing information with an entity that is not subject to the *ATIPPA, 2015*.

Information is collected for a specific purpose and individuals provide their information for this reason. When disclosing this information to another entity with different mandates and purposes, it is important to bear in mind the reasons for originally collecting the information.

It is also important to remember that, while legislation may authorize information disclosure, in very few cases is disclosure mandatory. In the majority of cases, access to the information is a privilege, not a right, and the decision to provide access is a discretionary one. Entities seeking information must ensure that appropriate safeguards are in place and, in the event of non-compliance, understand that disclosure may cease. Access to information, especially information collected from a source other than the individual the information is about, is a benefit.

In order to document best practices, this Office identified a database containing personal information of a large number of residents. Service NL's Motor Registration Division (MRD) database impacts every resident of the Province with a driver's license or vehicle registered in their name. It is not uncommon for other entities to be interested in information contained in databases like the one developed by the MRD.

Service NL has entered into a number of ISAs to provide external entities access, directly or indirectly, to the information contained in the MRD database. ISAs are in place with a variety of public bodies as defined by the *ATIPPA, 2015*, several insurance companies, and a number of federal entities. MRD had agreements in place with most entities to which it discloses information.

This Report outlines legislative requirements, presents findings from the audit and discusses key observations and recommendations. The Department was notified of this Office's intent to audit in December 2016 and the audit was conducted between February and June 2017. The audit started with background research and a review of documents supplied by MRD. In March, representatives from the OIPC attended a system demonstration at MRD in Mount Pearl. Various levels of access were demonstrated during this session to mimic some of the access available to external users. Once copies of the ISAs were reviewed, several agreements were selected for compliance follow-up. The follow-up was either conducted by the MRD or OIPC directly.

While areas for improvement were identified, MRD demonstrated that safeguards were in place to protect the information contained in the system. During the course of the audit, several areas were identified for improvement. This Office was encouraged to see agreements in place with most entities. Further, the agreements were of increasing quality, with the most recent agreements some of the best. Instead of waiting for the final audit report, Service NL representatives immediately started working to address identified gaps, such as having a consistent ISA template used for all agreements. As a result, an updated ISA template is nearing completion and affiliated application processes are now documented to better ensure consistency.

Despite MRD safeguards, follow-up on compliance with the agreements revealed concerns. It is important to note that this follow-up establishes the expectations of this Office when critically analyzing compliance with both the *ATIPPA, 2015* and applicable ISAs. One public body was found to be using the information for a number of unauthorized purposes and one staff member used the system for non-work related reasons. This type of activity is unacceptable.

The ISA renewal provides an opportunity to ensure compliance with the agreements. Prior to renewing any agreements, MRD should ask for a specific activity report (for those agreements that require it) for each year of the agreement, as well as the training log and details of the training provided (for those agreements that require it) for select years of the agreement.

MRD demonstrated that they provided access to the minimum necessary information for the receiving entity to accomplish its identified purpose. For example, although one agreement provides access to the driver's license number, it was determined that only the initial digits were required. As a result, those end users do not have access to the last three digits.

MRD, like many entities, works within the confines of a legacy system. Creating activity reports is time consuming, yet MRD recognizes the importance of such reports and has made them a priority. While it is not practical to recommend replacing the existing system, one recommendation in this Report is to ensure that robust auditing requirements are included in any RFP or Tender issued for system upgrades or replacement.

Overall, the audit revealed many strengths. For the most part, ISAs are in place. While the ISAs could be strengthened, they provide a solid foundation for the information sharing. Throughout the audit, MRD representatives were responsive and quick to take initiatives to address identified gaps.

Challenges include working with a legacy system and resistance by some public bodies to provide the necessary information to MRD. When one public body discloses information to another, the receiving public body has a responsibility to provide information to the source

to ensure compliance with legislation and other expectations. If the receiving entities do not fulfill their reciprocal obligations, they should gather the information from elsewhere.

This Report concludes with recommendations to address the identified challenges and the public body's response to these challenges.

Introduction

The Office of the Information and Privacy Commissioner of Newfoundland and Labrador (OIPC) provides independent oversight of the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) and the *Personal Health Information Act* (*PHIA*) and related regulations.

The OIPC's Audit and Compliance Program includes evaluating the adequacy of public body safeguards to protect personal information and comply with the *ATIPPA, 2015*. Audits are conducted under the authority of section 95(1)(b) and section 95(3) of the *ATIPPA, 2015*. Section 95(1)(b) empowers the Commissioner to *monitor and audit the practices and procedures employed by public bodies in carrying out their responsibilities and duties under this Act*. Section 95(3) extends the Commissioner's investigative powers established elsewhere in Part IV to other activities, including audit.

Citizens expect the OIPC, as the oversight body, to assess the level of compliance with the law, to advocate for best practice and to assist public bodies in establishing effective privacy management programs.

This audit examines the Information Sharing Agreements (ISAs) used by the Motor Registration Division (MRD) when providing access to the MRD database to other public bodies. The audit examines the:

- purpose for the information sharing;
- authorities for the information sharing;
- information that is being shared;
- safeguards in place; and,
- adequacy of the content of the agreements.

Service NL is responsible for the MRD. MRD is responsible for driver and vehicle safety through a number of programs and services, including driver licensing and vehicle registration. The Division also issues photo identification cards to the general public.

There are a number of reasons why the OIPC selected the MRD for audit. The MRD database impacts every resident of the Province with a driver's license or vehicle registered in their name. While some of the personal information located in the MRD would not be considered particularly sensitive, the number of citizens impacted and the fact that some medical information is collected makes it a system of interest.

Over the years, our Office has received a number of privacy complaints and breach reports involving the MRD. During the resolution processes associated with those breaches, the MRD has made commitments to make changes and improve information handling practices. This audit provides an opportunity to follow-up on some of the recommendations and to assess the ISAs in place.

The Department was notified of this Office's intent to audit in December 2016 and the audit was conducted between February and June 2017. The Department embraced the opportunity and provided all requested information in a timely fashion. The level of cooperation from the Deputy Minister to frontline staff was exemplary.

Audit Objectives

The objectives of this audit are to:

- assess whether the MRD has implemented adequate safeguards to protect the personal information in its custody or control when providing other public bodies with access;
- determine whether its processes for safeguarding the information comply with the requirements of the *ATIPPA, 2015;*
- establish considerations for information sharing agreements that all public bodies and businesses can use when determining what is reasonable for the information in their custody or control;
- review the extent of compliance with the ISAs; and
- where appropriate, make recommendations to strengthen policy or practice.

The purpose of this Report is to document best practices in ISAs, and to review and recommend improvements for the Division's ISAs, taking into consideration the public body's obligations under the *ATIPPA, 2015*. The Report outlines legislative requirements, presents findings from the audit and discusses key observations and recommendations.

Audit Focus

This audit examined public bodies that have been provided with access (direct and indirect) to the MRD database to collect information about individuals. While the MRD directly collects the information contained in the database from individuals, for other public bodies accessing the MRD database, this represents an indirect collection. An indirect collection occurs when personal information is collected from someone other than the person the information is about.

This audit did not examine entities that regularly request information from MRD with consent, such as law firms on behalf of clients, insurance companies, or employers seeking driver abstracts regarding employees tasked with driving as part of their work. It also did not examine federal entities with access to the MRD database, including the Royal Canadian Mounted Police, Statistics Canada, or the Canada Revenue Agency. Many of the audit's conclusions are relevant to the access that some of the above have to the MRD.

Audit Process

This audit was conducted in accordance with the legislative mandate and practices of the OIPC, and is based on the standards recommended by the Canadian Institute of Chartered Accountants (CICA).

The OIPC has adopted the Generally Accepted Privacy Principles (GAPP) that form the foundation for the Privacy Maturity Model developed by the American Institute of Certified Public Accountants (AICPA) and the CICA as the standard against which audits will occur.

The audit started with background research information and a review of documents supplied by MRD. In March, representatives from the OIPC attended a system demonstration at MRD in Mount Pearl. Various levels of access were demonstrated during this session to mimic

some of the access available to external users. Once copies of the ISAs were reviewed, several agreements were selected for compliance follow-up. The follow-up was either conducted by the MRD or OIPC directly.

Overview of ATIPPA, 2015

Many aspects of the *ATIPPA, 2015* must be considered when disclosing personal information, even if the disclosure is to another public body. Section 3 of the *Act* establishes, in part, that individuals have a right to be protected from the unauthorized collection, use or disclosure of personal information by public bodies. Section 64 establishes expectations regarding the protection of personal information. ISAs are a commonly used administrative safeguard when information sharing occurs.

Generally, a public body allowing third parties access to its information employs an ISA to document privacy considerations and to demonstrate compliance with the requirements of the *ATIPPA, 2015*. The two main parties to an ISA are normally:

- The source of personal information (the party disclosing the information). The ISA is designed to protect the information once it is disclosed.
- The recipient of personal information (the party indirectly collecting the information). The recipient must comply with the requirement of and restrictions in the ISA, which should include limitations on access, collection, use and disclosure, as well as explicit safeguards for audit, training and retention.

The source of the information needs to establish its authority to disclose the information. Section 68(1) sets out the authority for a public body to disclose personal information and 68(2) states that the disclosure should be the minimum amount of information necessary to accomplish the purpose for which it was disclosed.

Section 62(2) requires that public bodies tell an individual from whom it collects personal information the purpose for the collection, the legal authority for collecting it and contact details for an employee that can answer questions about the collection. The source of the

information should also review any privacy notices to determine if revisions need to be made to reflect the new disclosure.

The public body receiving the information must establish its authority to indirectly collect the information. Sections 61 and 62 address collection and indirect collection. In addition, the recipient needs to consider the authority to use the information, which is addressed in section 66.

Section 63 requires public bodies to make every reasonable effort to ensure that the information is accurate and complete when the information is being used to make a decision that directly affects the individual.

Section 64(1) requires that personal information be protected, stating:

> *64. (1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that*
>
> *(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;*
>
> *(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and*
>
> *(c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.*

Section 64(3) requires the head of the public body that has custody or control of the personal information to notify the individual who is the subject of the information when the information is stolen, lost, disposed of (except as permitted by law) or disclosed to or accessed by an unauthorized person.

Section 64(4) requires the Commissioner to be notified of any breach involving the unauthorized collection, use or disclosure of personal information.

Section 65 establishes retention requirements. If personal information is used to make a decision that directly affects the individual, the information must be retained for at least a year.

Information Sharing Agreements (ISAs)

ISAs are an essential administrative safeguard used to assist the source of the information to ensure compliance with the *ATIPPA, 2015*. Before entering into an ISA, it is important for the source to ensure that the expectations of individuals from whom the information was collected are respected. Statements regarding the reason for the collection and any subsequent use and disclosure need to be adhered to.

ISAs are discussed in Report F10-02 by former British Columbia Information and Privacy Commissioner Paul Fraser:

> *C. Information-Sharing Agreements*
>
> *[118] To be FIPPA compliant, public bodies must use information-sharing agreements to govern the disclosure of personal information from one entity to another. An information-sharing agreement sets out the terms and conditions for how the personal information will be collected, used, and disclosed by the entity receiving the data. Information-sharing agreements also enhance the transparency and accountability of public bodies with respect to data flows of personal information and how the privacy of individuals is being protected. Government recently recognized their fundamental importance in a statutory requirement for information-sharing agreements with respect to disclosures from health information banks [E-Health Act, s. 19].*
>
> *…*
>
> *[120] We conclude that there are information-sharing agreements in place for most external disclosures but that they do not always impose specific or detailed standards for the protection of the privacy and security of personal health information. The agreements should not merely reference broad legislative standards, but specifically state the obligations of the recipients of the data to protect it. Given the particular sensitivity of personal health information, all information-sharing agreements should specify high standards for privacy and security, including encryption, secure storage, retention schedules, and requirements for secure disposal of personal information.* [emphasis added]

There are many benefits to ISAs. The Government of Canada's Guidance on Preparing Information Sharing Agreements Involving Personal Information states:

The benefits of using an ISA include:

- *clarifying the rights, obligations and accountability of the parties;*
- *ensuring compliance with applicable privacy protection legislation and policies;*
- *defining custody and control issues;*
- *limiting use and disclosure;*
- *establishing protocols for addressing problems and incidents;*
- *providing awareness and instructions for staff;*
- *ensuring transparency for affected individuals.*

It is important to consider the standards established regarding ISAs when assessing whether critical content is included in the agreements at hand; not every consideration for an ISA is mentioned below. Our review of documents, both those provided as part of the MRD submission and those obtained through our own research, identified some critical content that should be included in agreements entered into by MRD. While all agreements must include fundamental safeguards, each agreement will be unique and may require additional considerations.

General Components of Information Sharing Agreements (ISAs)

Resources available to any entity considering an ISA include:

- Model Data Sharing Agreement published by the Information and Privacy Commissioner of Ontario
- Guide for Developing Personal Information Sharing Agreements published by the Access and Privacy Division of Service Alberta
- Best Practices for Information Sharing Agreements, published by the Information and Privacy Commissioner of Saskatchewan

ISAs should include the following details:

- The name of all parties to the Agreement.
- A concise statement as to purpose - why does the information need to be shared? What is the reason for the agreement?

- Description of the personal information - what is being disclosed? Why is each piece of information necessary for the identified purpose? Only those fields of personal information that are clearly necessary to achieve the identified purpose should be shared.
- Method of information sharing - how will the information be shared? What safeguards are in place to ensure the information is protected in transit and at rest?
- Use - how will the information be used? The acceptable uses should be clearly defined in the agreement, ensuring all parties understand what will constitute a breach of the agreement. These acceptable uses could then be used for employee training purposes.
- Disclosure - will the recipient disclose the information to third parties? Any subsequent disclosures should be identified in the agreement, along with the authority for the same.
- Authority - under what legal authority is the information collected, used and disclosed? The agreement should be specific, for example, naming the sections and subsections of legislation that authorize the sharing. The source of the information must cite the authority to disclose and the recipient of the information must cite the authority to indirectly collect the information. This should not be restricted to the *ATIPPA, 2015*; other legislation may establish the authority for the information sharing in conjunction with the *ATIPPA, 2015*.
- Access - who will have access to the information once it is disclosed? This should be restricted to those who need access to accomplish the identified purpose. The process for obtaining access should also be identified. For example, will an application form be used? The agreement should also identify notification responsibilities and expectations if an individual with access leaves the entity.
- Safeguards - what administrative, technical and physical safeguards are expected and required to protect the information from unauthorized use or disclosure? For example, how will access be restricted to authorized individuals? If it is electronic access, the expectation that each user have a unique account should be established.
- Breach - the agreement should require the reporting of all privacy breaches to the source. The requirement should address breach of the agreement, as well as of the

ATIPPA, 2015. If it is a breach under section 64(4) of the *ATIPPA, 2015*, responsibility to notify the OIPC should be clearly noted. This section should also identify the consequences of breaches, up to and including the termination of the agreement and/or suspension of access for individual users.

- Activity Reports - activity reports (audits) should be required and the agreement should identify the roles and responsibilities of each party regarding the same. The scope, frequency and certification of activity reports must be outlined in the agreement. The consequences of non-compliance should be clearly stated.
- Training - what training expectations are in place and what are the roles and responsibilities of each party? At a minimum, those with access should be aware of the acceptable use of the information.
- Custody and control – clearly identify who has custody and control of the information at various stages of the information sharing. Identify the roles and responsibilities of the parties to the agreement regarding the same.
- Retention and Destruction - detail any specific retention requirements and expectations for secure destruction.
- Timeframe - the agreement should have a beginning and end date; the agreement should be reviewed and updated as needed before renewal. Either party should be able to immediately terminate the agreement if circumstances warrant.
- Changes - the parties should advise if any changes that affect the agreement occur, such as a change in policy or procedures.

Additional Considerations

When a public body is sharing information with another public body, both entities are subject to the *ATIPPA, 2015*. However, a public body may enter into an ISA with a private entity that is not subject to *ATIPPA, 2015*. It is important to ensure that adequate safeguards are in place. For example, a private entity is not required to comply with *ATIPPA, 2015,* however it may be subject to other similar laws such as the *Personal Health Information Act (PHIA*) or the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). The agreement should establish expectations on issues such as reasonable safeguards and reporting of breaches.

Motor Registration Division (MRD)

The mandate of the MRD, according to the 2014-2017 Strategic Plan for Service NL, is as follows:

> *The Motor Registration Division (MRD) is responsible for driver and vehicle safety through a number of programs and services, including: driver licensing and vehicle registration; driver examinations; highway enforcement and weigh scales for commercial vehicles; driver records (convictions, suspensions, accident and medical records); and collection of taxes on vehicle sales, court fines and other government revenues. The Division also issues photo identification cards to the general public.*

As of 2013, there were 377,840 licensed drivers in the province, with 814,921 registered vehicles (including cars, trucks, snowmobiles, ATVs, trailers). Motor Vehicle Registration had a total number of 1,546,366 transactions in 2014.

The MRD has entered into ISAs with various entities, including some core government departments, municipalities, law enforcement agencies, private insurance companies and federal entities. The ISAs allow direct and indirect access to the MRD database by the external entities.

The MRD System

The MRD database was created for the collection of information necessary for the issuance of driver's licenses and vehicle registrations as per sections 10, 40, 43 and 74 of the *Highway Traffic Act* and to make use of information technology to improve business processes. The database has information fields under three categories: vehicle inquiry, driver inquiry and driver records medical inquiry. The majority of the information contained in the system is personal information as defined in the *ATIPPA, 2015*.

The *Highway Traffic Act* allows MRD to disclose information contained in the database:

> *6 (1.1)Where information contained in driver or vehicle records, or of an entry in those records kept in the division, is requested, a copy of the information contained in the record may be released to*

> *(a) other government departments or agencies of the province, a municipality, the Government of Canada, the government of another Canadian jurisdiction, or the government of a state or country, to ensure compliance with a statute or order;*
>
> *(b) research groups, market analysis companies, study groups and similar organizations, where the information is not to be used for solicitation purposes;*
>
> *(c) motor vehicle manufacturers or other agents for recall of defective motor vehicles; or*
>
> *(d) another individual, group or agency where in the opinion of the minister the release of the information is not contrary to the public interest.*

It is important to examine the safeguards Service NL has in place for its own staff accessing the MRD database, as it is reasonable to expect external entities seeking access to have the same or higher levels of safeguards in place. Service NL staff, including those working in the MRD, are subject to a Privacy, Confidentiality and Security of Information Policy. Staff are required to sign this document, after it has been reviewed with their supervisor and they have had the opportunity to ask questions. They also complete the ATIPP Online training, described as follows:

> *This module is intended to give participants an understanding of their responsibilities as public body employees to uphold access and privacy provisions. This is done by providing an introduction to access and privacy principles and Newfoundland and Labrador's Access to Information and Protection of Privacy Act (ATIPPA).*

Before system access is provided, staff receive training on how to use the database.

As the database contains a large volume of information, there are a number of safeguards in place. There are defined levels of system access and each end user has a unique user ID. When a new user is provided with access, an established process is used to communicate their unique user name and password.

While all end users will see all information field labels, only those fields they are authorized to view are populated. Further, if an end user selects a screen they are not authorized to access, they are notified by the system that, “You are not authorized to access this option.” A limited number of end users are able to update fields with the remainder limited to viewing

privileges only. End users are able to print a copy of the information, take a print screen shot, and copy and paste information. The information cannot be exported directly into a spreadsheet.

Those with access are able to search using any of the information fields to which they have access, such as name and license plate. When searching by name, similar matches appear on screen and the correct individual is located and selected by virtue of other identifiers.

While there is no formal auditing program in place, the system does capture all activities of end users and MRD runs regular access activity reports. Disciplinary action has been taken against employees for inappropriate access discovered through activity reports and there are breach protocols in place to address situations involving inappropriate access.

The system has a variety of technical safeguards in place; the safeguards most relevant to this audit involve the activity levels of accounts. Accounts that have been inactive for an established period of time have the password suspended; users must be re-approved by MRD before the account is reactivated. Accounts that remain inactive are automatically deleted after an established period of time. MRD also reviews activity reports and identifies users that have not accessed the system recently; they then make contact to determine if access is still required. In addition, the system will timeout after a period of inactivity.

Access to MRD by External Entities

It is not uncommon for other entities to be interested in information contained in databases like the one developed by the MRD.

Service NL has entered into a number of ISAs to provide external entities access, directly or indirectly, to the information contained in the MRD database. ISAs are in place with a variety of public bodies as defined by the *ATIPPA, 2015*, several insurance companies, and a number of federal entities. These agreements facilitate access for approximately 325 end users. No agreements are in place with the Royal Newfoundland Constabulary, although 269 of its staff have direct system access, or the Royal Canadian Mounted Police, with 203 staff with direct system access. All public bodies with access to the MRD database are listed in Appendix A.

Once an ISA is in place, new users can be added through one of two processes. For entities on the government network, new users must complete the Request for Access to the MRD-MIS Computer System (Internal Departmental Requests). The form seeks details on a number of things, including why access is being requested, the information required, the number of individuals that will require access, if consent will be sought prior to accessing individual files, and if information will be disclosed to any other individuals or entities. New users in entities outside the government network must complete the Remote Access Request Form, which gathers information regarding the user and the asset that will be used to access the database. Both MRD and the OCIO use the information to process the request and establish access.

During the access process, entities are asked to identify the information fields to which they request access; no external entities are able to access medical information. This helps ensure that access is limited to include only the information fields necessary to accomplish the identified purpose. When it comes to external entities accessing the system, MRD sometimes determines that full information field access is not required. For example, although one agreement provides access to the driver's license number, it was determined that only the initial digits were required. As a result, those end users do not have access to the last three digits. In addition, while the vehicle owner can be viewed, it is only the primary owner that is seen by most users, even if there are multiple owners.

No external entities are able to modify or add information. Each individual within an organization has unique credentials (user name and password).

Some of the more recent ISAs address auditing, requiring Service NL to provide a monthly activity report to the receiving entity; entity representatives are expected to review and sign off on the reports confirming that there have been no unauthorized accesses or disclosures of personal information. While Service NL does not require that these reports be returned, they do reserve the right to audit the same with notice.

Observations and Recommendations

Application Process for Access for External Entities

The information contained in the MRD database was collected for a specific purpose and individuals provided their information for this reason. When considering providing access to external entities with different mandates and purposes for the access, it is important to bear in mind the reason the database exists. While legislation may authorize MRD to disclose the information, in very few cases is this disclosure mandatory. As such, in the vast majority of cases, access to the information contained within this database is a privilege, not a right, and the decision of MRD to provide access is a discretionary one.

Further, while some entities may have the authority to collect the information involved, if the information is obtained through MRD, it is an indirect collection. Section 62 of the *ATIPPA, 2015* addresses collection and limits indirect collection to specific circumstances.

Through the course of this audit, MRD indicated that a Court decision (*R. v. Unnamed Defendant*, 2013 NLPC 013081316) has impacted work flow and has led to more external entities, especially municipalities, seeking direct system access. In response, while not formally reflected in policy, MRD has added volume of requests to screening criteria to determine if a public body requires direct access to the database or should be limited to indirect access. One agreement reviewed during this audit provided indirect access to the public body, with representatives calling MRD to obtain information.

End users with direct access are able to query the system directly; end users with indirect access must contact MRD and provide details on the request to the appropriate representative. Once this information is collected, the representative will search the system and provide the entity with the requested details.

Recommendation

> MRD review its collection notice to ensure it reflects the disclosures that occur under the ISAs.

Public Body Response:

MRD accepts this recommendation. MRD will review its collection notice to ensure it reflects the disclosures that occur under the ISAs.

Recommendation

MRD formalize the application process through procedure or other documentation. The process should include screening criteria to determine if direct or indirect access is the most appropriate in the given circumstances.

Once the initial screening process is complete, entities should be required to provide the following to MRD:

- The reason why access is required / the purpose for the access.
- The specific legislative authority for the indirect collection (please note that current ISAs may include the legislative authority, but are not in and of themselves the authority for the collection).
- A table with two columns. The first column should list all information fields to which access is required and the second should explain why access is required for the specific field.
- Any supporting documentation requested by Service NL. This could include, but not be limited to, municipal regulations, privacy policies, details of privacy training, etc.
- The names, titles and/or position descriptions of all end users being provided with access.
- If multiple personnel are intended to have access, justification from an operational perspective for providing access to multiple personnel (convenience is insufficient).

Public Body Response:

MRD accepts this recommendation. The Director of Information Management is working with the Deputy Registrar of MRD on Guidelines to be followed prior to entering into an ISA with any entity. The new ISA template will require a detailed explanation of the purpose for access; the specific legislative authority for the indirect collection of the information by the entity; the Appendix will include a two columned table that will list all information fields to which access is required and the explanation as to why access is required for the specific field; the Appendix will also list the titles of all end users being provided with access. Discussions with the entity prior to accessing the MRD system, either directly or indirectly, will determine if multiple personnel will be granted access.

Information Sharing Agreements (ISAs)

Service NL provided a number of information sharing agreements to this Office for review; the focus of this audit is on ISAs with public bodies within Newfoundland and Labrador. Commendably, MRD had ISAs in place to address the majority of the accesses provided to external entities. A notable gap is in the lack of agreement with law enforcement agencies. This is of particular concern to the OIPC given our knowledge of three breaches of the MRD database by Royal Newfoundland Constabulary (RNC) personnel since 2015. While the authority for MRD to disclose the information is established in legislation, the ISA is a critical safeguard presently missing. MRD's obligations to protect the privacy of its personal information holdings requires due diligence on its part to make every reasonable effort to limit potential breaches by external entities it provides with access.

MRD has attempted to enter into an agreement with the RNC in the past and, in January 2017, this Office suggested that the RNC enter into an ISA with MRD. Activity reports have been regularly provided for review since the end of 2015. In June 2015, MRD noticed potentially inappropriate accesses and contacted the RNC regarding the same. Two other breaches have been reported to this Office involving RNC access to the MRD, both of which

were intentional. One was discussed in Report P-2015-002 and the other lead to a prosecution which is currently before the Courts. The RNC provided no notification of these breaches to MRD.

This Office noted some inconsistencies in the agreements and identified areas for improvement. In many cases, this reflected improvements made to the template over the years, with the most recent agreements being much stronger. With many agreements up for renewal in the next six months, this Office provided detailed feedback early in the audit process so Service NL could commence work on further improvements to the ISA template. It is our understanding that a new template is in an advanced stage of development, with progress impacted by a number of retirements in key areas. As a result, the majority of agreements have been extended and renewals will be signed by the end of 2017.

Areas identified for improvement in the agreements include:

- The identified purpose is not always clear. It is difficult to critically analyze the reason for the access and the information fields requested without a clear purpose.
- While the authority for MRD to disclose the information is generally well-stated, the legislative authority for the recipient to indirectly collect the information is generally lacking.
- Where legislative authority is cited, specific sections and subsections are often not identified.
- The names of the information fields listed in the agreements are not consistent.
- All schedules listing the information the entity will access should explain why each information field is required; only one agreement contained this level of detail. All access to information fields should tie directly to an identified purpose.
- Agreements do not identity what constitutes an inappropriate use of the system or state the consequences of such activities. The agreement does restrict access, use and disclosure to the purposes stated in the Agreement. However, many of the purposes stated in the agreements are not clear. Service NL does have the ability to immediately cease access to the system by individual users or entities.

- Agreements should all require system specific training, including details of acceptable system use. Several agreements contain the following language:

> *[receiving entity] agrees to ensure that all employees, agents or contractors with access to the information received under this Agreement will be provided with appropriate training related to the confidentiality, protection and approved disclosure of this information, upon initial approval and at a minimum, annually thereafter. Records of this training will be maintained by [receiving entity] and will be made available to Service NL upon request.*

- All agreements must have robust audit requirements. Some agreements require Service NL to print and send monthly activity reports to the entities for their review and sign off, with some agreements further explaining the purpose for the audit as, "…to ensure that information was not used for non-work related purposes (i.e. employees searching own records, records of family and friends, etc.)." All agreements should reflect these additional clauses in the audit section. All agreements should contain language regarding appropriate and inappropriate use.
- Agreements require that breaches of the agreement be immediately addressed and notify Service NL of same. As section 64(4) of the A*TIPPA, 2015* requires that all breaches be reported to the OIPC, agreements should clearly identify the entity responsible for reporting the breach to this Office.
- The agreements should contain language that addresses consequences of non-compliance.
- The agreements do not mention any requirement to notify Service NL if staff with access depart or change roles. This is most important if staff have remote access through a personal device.
- Service NL should consider if additional action is required if end users are disciplined or terminated for inappropriate handling of personal information, either related to the MRD access or other systems. For example, the entity could closely monitor the activities of that end user in the MRD system for the past 12 months.

The ISA renewal provides an opportunity for Service NL to ensure compliance with minimal effort. Prior to renewing any agreements, Service NL should ask for a specific activity report (for those agreements that require the same) for each year of the agreement, as well as the

training log and details of the training provided (for those agreements that require the same) for select years of the agreement.

As with any agreements that have been in place for a period of time, there are also general content updates to be considered. For example, some of the older agreements reference an older version of the *ATIPPA* that has been replaced by the *ATIPPA, 2015*. In addition, the name of some entities has changed and/or divisions have moved to different Departments under government restructuring. The latter emphasizes the importance of having ISAs with Divisions or core government departments and not umbrella agreements. For example, there is an agreement with the Department of Justice and Public Safety that involves the Fish and Wildlife Enforcement Division; according to a government news release on government structure realignment issued February 22, 2017, this Division is now under the new Department of Fisheries and Land Resources.

Recommendation

> Develop an updated ISA template that better reflects best practice and the areas identified for improvement. This new template should be used for all agreements upon agreement renewal.

Public Body Response:

MRD accepts this recommendation and is in the process of creating a new ISA template which will be completed by October 31, 2017.

Recommendation

> Once the updated ISA template is available, immediately commence work on an agreement with the RNC. If no agreement is in place by October 31, 2017, all access by RNC to the MRD database should be terminated. Access should only be restored upon the conclusion of an agreement satisfactory to MRD.

Public Body Response:

MRD accepts this recommendation. The Deputy Registrar of MRD will contact the Director, Information Management for the RNC and inform her that an ISA must be signed by October 31, 2017 or the RNC's access to the MRD system will be terminated.

Recommendation

During agreement renewal, ensure all entity names are updated to reflect current names and that each Division of core government departments have unique agreements. Ensure all references to legislation are current.

Public Body Response:

MRD accepts this recommendation. The new ISA template will ensure all entity names are updated to reflect current names and that each Division of core government departments will have unique agreements and will ensure all references to legislation are current.

Recommendation

Service NL establish the expectation of a "mini audit" upon agreement renewal in the agreement itself.

Public Body Response:

MRD accepts this recommendation. The ISA Guidelines will include a section directing that a "mini audit" be completed upon agreement to renew the ISA and the ISA itself will reflect that a mini-audit will be completed prior to renewal.

Compliance with ISAs

This Office initiated follow-up on select Agreements to determine if any compliance issues existed. Some follow-up was done by MRD, other follow-up was done directly by this Office. Overall, the results were encouraging. It is important to note that this follow-up establishes the expectations of this Office when critically analyzing compliance with both the *ATIPPA, 2015* and the applicable ISA.

Transportation and Works

Many of the ISAs are with core government departments. After requesting audit reports for a 12 month period from MRD, this Office followed-up directly with the Department of Transportation and Works to gauge compliance with the ISA. The ISA states, in part:

> *This Information Sharing Agreement (ISA) will provide for the disclosure of personal information from Service NL to the Department of Transportation and Works (Department of TW) for the purpose(s) of:*
>
> *Validation of driver licenses for government employees operating Government of Newfoundland and Labrador vehicles;*
>
> *Confirmation of vehicle registration of government-owned vehicles; and*
>
> *Cross-referencing outstanding fines by government department for invoicing and payment purposes.*

Further, the ISA requires that the Department review a monthly activity report, sign and date the same, and report any instances of non-compliance to MRD.

Our review discovered several instances of non-compliance with the agreement. While the managers reviewing the audit reports were not aware of the requirement to sign and date them, the Department indicates that the reports were duly audited. Once this gap was identified, the Department indicated it developed a procedure, effective immediately, that requires signed and dated audit reports to be placed in its electronic document management system.

In addition, the Department was using its access outside of the purposes identified in the agreement, for example:

- Confirmation of vehicle registration for all Government vehicles operated or leased (not just owned) as defined by the Department of Finance.
- Determination of the registered owner of vehicles purchased by Government agencies, boards, commissions and municipalities under GNL's Standing Offer Agreement to notify the entity of recalls or service notices received by Transportation and Works.
- Determination of the registered owner of vehicles parked and/or abandoned on provincial highways, GNL parking lot access roads or parking lots or committing parking violations in GNL parking lot access roads or parking lots in contravention of the *Highway Traffic Act*.
- Obtaining detailed information on vehicles confiscated by GNL to allow court ordered disposal.
- Determination of the registered owner of vehicles sold to the public by GNL to notify the individual and/or company of recalls received by TW.

The Department determined that several of the unauthorized uses were more of an additional public service than a mandate of the Department and has indicated it will stop using the system for these reasons. For the others, the Department has indicated its intention to request that MRD consider these additional uses in a new ISA.

The audit also demonstrated that one end user accessed their personal vehicle information over a number audit reports. The Department noted that the end user had just sold their personal vehicle and was checking to see if the new owner had transferred ownership. That same end user accessed the same information on February 23, June 6, June 17, July 18, September 1 and September 14. The Department's submission, "…acknowledges that this was not addressed until further review was completed as part of this audit process." The Department has committed to promptly reporting any future breaches to both MRD as required by the ISA and to this Office as required by section 64(4) of the *ATIPPA, 2015*.

Recommendation

Until such time that the ISA is signed, this Office recommends that all accesses by the Department of Transportation and Works not addressed by the agreement or a Court Order immediately cease. As part of this process, MRD should review user accounts to ensure that only those requiring access for the reasons identified in the agreement have access. MRD should notify the Department in writing of all acceptable uses and end users resulting from this recommendation. Further, once an updated agreement is ready, compliance checks should be conducted on this Department by MRD.

Public Body Response:

MRD accepts this recommendation. MRD has had discussions with the Department of Transportation and Works (TW) and there has been an exchange of letters amending the department's purpose for accessing MRD information until the new ISA template is implemented. Access of the MRD system for purposes not included in the ISA, the amending letter or by Court Order by TW has ceased. MRD's Manager of Strategic Planning and Evaluation will review TW's user accounts to ensure that only those requiring access for the reasons identified in the agreement and amending letter have access to the system. TW will be notified in writing of all acceptable uses and end users resulting from this recommendation. Once the new ISA has been signed with TW, MRD will conduct quarterly compliance checks of the department until, at least, October 31, 2018.

Recommendation

> Upon agreement renewal, ensure entities have listed all uses for the information in the ISA.

Public Body Response:

MRD accepts this recommendation. The new ISA template and Guidelines will ensure that detailed explanations are provided from entities requesting access.

Municipalities

Many agreements with municipalities referenced municipal regulations as the authority for indirect collection. In addition, there was a wide variation in the number of users. These two areas were selected for follow-up and this Office identified agreements for specific review.

The Town of Grand Falls-Windsor has indirect access to the MRD. Each time they require information from the database they contact a representative of MRD. With only 23 requests for information between May 2016 and March 2017, indirect access is most appropriate for this entity. In addition, MRD verified that its representatives were in compliance with the expectations of the agreement, for example confirming that the individual requesting the information was an authorized representative of the Town.

The ISA with the Town of Paradise referenced Town regulations in general and this Office sought clarity of the authority for the access. MRD followed-up with the Town and provided this Office with the specific regulations being enforced. When municipal regulations establish the authority for the municipality's indirect collection, it is important to obtain copies of specific regulations to attach to ISAs and provide specific details in the agreement itself.

The number of users with system access varied among municipalities, from 1 user to 25. The OIPC has concerns that entities with one user may be sharing accounts, so it was

suggested that this be included in any future ISA template; end users should not share accounts. Accounts are assigned to individuals and these individuals are accountable for all actions related to their account on the system. This Office followed-up with the City of St. John's, as the municipality with the highest number of users with 25 accounts. This Office requested from Service NL the list of all staff with the City of St. John's with access. We then contacted a City representative and requested titles for these individuals. Of the listed active end users, four were retired and one had left the organization.

The identified purpose for access documented in the ISA states:

> *Release of vehicle licence and record information and associated name and address of registered owner(s) of the vehicle(s) to the City of St. John's to assist the City of St. John's with Parking Enforcement and Traffic Operations.*

Many of the end users worked in parking enforcement or in the prosecution of tickets. However, a number of users with the City hold the title of "Customer Service Representative" and the Manager indicated that they use the access to process permits for Robin Hood Bay. This Office did not seek a formal submission from the City on this matter, as it is not the specific focus of this audit. However, at face value this use does not appear to be addressed in the above purpose nor in the spirit or intent of the agreement.

Recommendation

During ISA renewal, including ISA renewal for the City of St. John's, review the names and titles of all individuals with access and cross reference this with the identified purpose for the access.

Public Body Response:

MRD accepts this recommendation. During ISA renewal MRD will review the names and titles of all individuals with access and cross reference this with the identified purpose for the access.

Recommendation

> Document the process for adding new users and identify the parties responsible for reporting staff changes that impact user accounts in the ISA.

Public Body Response:

MRD accepts this recommendation. The ISA Guidelines will Document the process for adding new users to the entity's access. The new ISA template will identify the parties responsible for reporting staff changes that impact user accounts in the ISA.

Recommendation

> Include the specific authority for the indirect collection in all agreements with municipalities. Applicable municipal regulations should be included in an Appendix to the agreement.

Public Body Response:

MRD accepts this recommendation. The specific authority for the indirect collection will be included in all ISAs with municipalities and applicable municipal regulations will be included in an Appendix to the agreement.

Audit Program

While activity reports are run by MRD on a monthly basis, there is no audit program in place. Such programs may proactively detect and deter inappropriate access and use of personal information, for example, red flagging a search by a user with the same address or last name. In addition, MRD staff indicate that the activity reports are time consuming to produce, requiring multiple steps to organize the data by user and import into an accessible

format. Hardware and software limitations currently preclude streamlining this process via information technology solutions.

It is interesting to note that, when MRD initially started to run regular activity reports and send them to external entities for review, some end users asked for their access to be disabled and a significant reduction in the number of system queries was noted. This highlights the importance of not only having audit features, but also of conducting regular audits on system access.

It is through reviews of activity reports that any inappropriate access will be identified. Robust audit programs deter end users from accessing the MRD for unauthorized purposes. While MRD is able to discipline its own staff for inappropriate system use, this does not extend to end users in other entities. However, MRD is able to control access to the system. In order to ensure that access is not abused and to ensure fairness, MRD should ensure that entities with access promptly review monthly activity reports for their own end users, notify MRD of any breaches and understand that MRD may suspend access to an individual user or the entire entity. In addition, ISAs should establish the expectation that end users are not able to review and approve their own system access.

Recommendation

> When, in the future, the MRD upgrades or replaces the current database, audit requirements and capabilities be included and clearly defined in the RFP/Tender.

Public Body Response:

MRD accepts this recommendation. When the MRD upgrades or replaces the current database, audit requirements and capabilities will be included and clearly defined in the RFP/Tender.

Recommendation

Establish the requirements for reviews of activity reports in the ISA template. For example, individuals should not be able to review and sign off on their own access. External entities should be required to conduct reviews of activity reports and to promptly report any concerns to the MRD. All ISAs should include a requirement for the recipient to confirm to MRD that the monthly activity report has been reviewed and no inappropriate access has been identified. While MRD should identify the most efficient way for this to occur, this Office suggests an email or signed form.

The agreement should emphasize that access may be terminated or suspended based on the actions of individual end users.

Public Body Response:

MRD accepts this recommendation. The new ISA template will include: requirements for reviews of activity reports; that the recipient confirm to MRD that the monthly activity report has been reviewed and no inappropriate access has been identified; the requirement that individuals not review and sign off on their own access; that external entities be required to conduct reviews of activity reports and to promptly report any concerns to the MRD; and the agreement will emphasize that access may be terminated or suspended based on the actions of individual end users.

Staff Training and Confidentiality Oaths

While Service NL trains its own staff and offers training to entities with access to the database, training requests are infrequent. MRD should require training to be provided to all end users of the system; it is imperative that end users understand their roles and responsibilities regarding their access to the information contained in the system. New users must also receive privacy training. Privacy training for all users should be updated annually.

Recommendation

> Develop an end user agreement template that must be customized by receiving entities and signed by all end users. It should be the receiving entity's responsibility to ensure that end users sign the agreement and all signed agreements should be available to MRD for audit upon request. These agreements should establish that MRD may revoke system access if inappropriate use is discovered, even if such action results in the individual being unable to complete the normal duties of their position.

Public Body Response:

MRD accepts this recommendation. The new ISA template includes an "Access Management Confirmation" form that must be signed by all users in an entity that will have access to MRD information under the ISA. An entity will be able to customize the "Access Management Confirmation" in consultation with MRD should it be necessary. The ISA states that MRD may revoke system access if inappropriate use is discovered, even if such action results in the individual being unable to complete the normal duties of their position.

Recommendation

> Ensure all ISAs include a requirement for identified training and tracking of the same. External entities should be required to certify that personnel have received required training prior to MRD granting access to the MRD database. External entities should also be required to certify that all personnel with access to the MRD database have received additional training at least once every year.

Public Body Response:

MRD accepts this recommendation. The new ISA template includes a requirement for all entities with access to information under the ISA to be provided with the appropriate training related to confidentiality, protection and approved disclosure of this information, upon initial approval and at a minimum yearly thereafter. Records of this training will be maintained by the entity and will be made available to Service NL upon request.

Conclusion

ISAs are a commonly used administrative safeguard to assist public bodies in compliance with section 64 of the *ATIPPA, 2015*, which establishes expectations regarding the protection of personal information. MRD had agreements in place for almost all instances of information sharing and, although improvements were recommended to the agreements, they represent a solid foundation for information protection.

This Office encourages every public body to review the standards discussed in this Report and to conduct internal reviews to determine their own level of compliance.

Donovan Molloy, Q.C.
Information and Privacy Commissioner
Newfoundland and Labrador

Appendix A: Public Bodies with Access to the MRD

Public Bodies

Please note that the names of Departments have been updated to reflect the realignment announced on February 22, 2017.

Entity	Expiry Date
Department of Finance (Insurance Division)	September 30, 2017
Department of Finance (Tax Administration)	September 30, 2017
Department of Advanced Education, Skills and Labour (Finance and General Operations)	March 31, 2020
Department of Advanced Education, Skills and Labour (Income and Social Support)	March 31, 2020
Department of Advanced Education, Skills and Labour (Student Loan Corporation)	March 31, 2020
Department of Transportations and Works	July 31, 2017
Department of Children, Seniors and Social Development	July 31, 2021
Department of Justice and Public Safety (Fish and Wildlife Enforcement)	July 31, 2017
Department of Justice and Public Safety (Fines Administration)	March 31, 2020
Department of Justice and Public Safety (Support Enforcement)	March 31, 2020
Workplace NL	July 31, 2017
Newfoundland and Labrador Housing Corporation	June 30, 2017
Town of Paradise	July 31, 2017
Town of Conception Bay South	July 31, 2017
City of Mount Pearl	July 31, 2017
City of Corner Brook	July 31, 2017
City of St. John's	July 31, 2017
Town of Grand Falls-Windsor (indirect access)	July 31, 2020
Royal Newfoundland Constabulary	No ISA in place