OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Audit of Physical Safeguards

Pensions Administration and
Group Insurance Division,
Human Resource Secretariat

June 23, 2016

Table of Contents

Page#

Executive Summary 1

Introduction 3

- Audit Objectives 4
- Audit Focus 5
- Standards 5
- Audit Process 6

Overview of Physical Safeguards 6

- What is Considered Reasonable? 7
- Standards 8
- General Physical Safeguards 8
- Fax Machines 9
- Printers 10
- Workspaces 10
- Outside the Office 11
- General Access 12
- Physical Location 12

HRS Initiatives 13

- About the Division 14

Observations and Recommendations 15

- Personal Information Collected/Personal Information Involved 16
- Education and Awareness 17
- Accountability 19
- Physical Space 20
- Policies, Processes, Procedures and Guidelines 23

Conclusion 25

Executive Summary

Citizens expect the Office of the Information and Privacy Commissioner (OIPC), as the oversight body, to assess the level of public body compliance with the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*). An essential element of this undertaking is to review best practices in order to assist public bodies in establishing effective privacy management programs. This process can occur in different ways, but in this instance it has taken the form of a privacy audit which is a tool available to the Commissioner under the authority of section 95(1)(b) and section 95(3) of the *ATIPPA, 2015*. An audit can be broad or narrow in scope. The purpose of this audit report is to document, describe, comment and recommend improvements regarding physical safeguards in one public body, taking into consideration the public body's obligations under the *ATIPPA, 2015*.

It is important to note that being the subject of an audit does not mean that a public body has done something wrong; it is a formal opportunity to assess compliance and identify areas for improvement so as to better avoid privacy risks in the future. While this Office had to select a public body as the focus for the audit, this report is less about that particular entity and more about physical safeguards in government in general. Public bodies should review this document to better understand our expectations and identify their own areas for improvement.

Under section 64 of the *ATIPPA*, *2015*, each public body is required to have reasonable physical, administrative and technical safeguards in place to protect the information in its custody or control. Since there is never a 100% guarantee that safeguards are sufficient and consistently applied, most public bodies choose to take a layered approach, using the three types of safeguards in an overlapping and complementary fashion.

Although there have been changes to the *ATIPPA* over the years and best practices have evolved, the standard for what is considered a reasonable physical safeguard has not really changed. It is expected that this will be one of the most mature areas to audit for *ATIPPA, 2015* compliance.

This audit started with background research, including the physical safeguard standards established by the Government of Newfoundland and Labrador and Commissioner's Reports from this province, as well as other Canadian jurisdictions. In addition to formal submissions, a site tour and staff survey were also conducted in the Human Resource Secretariat's (HRS) Pensions Administration and Group Insurance Division. This report outlines legislative requirements, presents findings from the audit, and discusses key observations and recommendations.

Overall, all expected physical safeguards were identified during the audit process. There was controlled access, storage areas with locks, and shredding for secure disposal of records. The staff survey demonstrated a solid awareness of physical safeguards, and documentation demonstrates proactive, continuous improvements in physical safeguards. The HRS has also produced several customized information protection publications. While general training is valuable, it is important to provide complementary training like this to assist staff in connecting broad concepts to their specific roles and daily tasks.

Two tools introduced by HRS should be considered for adoption by all public bodies: the Divisional Checklist for Monitoring Protection of Personal Information (Divisional Checklist) and the concept of teachable moments. The Divisional Checklist was designed to identify areas where breaches could occur and try to mitigate the risk by making it a teachable moment for respective employees, where possible. The checklist process involved random checks of garbage, shredding and recycle bins; checking to see if items were left behind on printers and fax machines; ensuring the office and Registry were locked at the end of the day; overall workspace checks; and filing cabinet checks. The HRS also established the concept of teachable moments, which highlights lessons learned from past breaches. These moments would discuss the breach and offer suggestions to avoid similar situations in the future.

Challenges include space constraints that impact file storage; this challenge could be addressed through a file digitization project as resources allow. As well, a sprinkler system is present in the Pensions Registry, which poses a risk to member files in case of fire and/or system malfunction. The Group Insurance Division is in need of a dedicated fax

line, as it is currently sharing with another Division. Overall, there is a need for improved documentation, including policies and procedures and a record of education activities.

It is encouraging to note that, during the course of the audit, the Division developed a comprehensive inventory of the information collected by and stored in the Division. This work was undertaken before this Office made any formal recommendations regarding the same. Proactive initiatives like these, designed to ensure compliance with the *ATIPPA, 2015*, provide a measure of confidence that such activities will continue in the future regardless of any potential reorganization of the Division or physical move of records should these occur.

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 involves evaluating the extent to which public bodies are protecting personal information and complying 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.

This first audit within the Audit and Compliance Program examines the reasonableness of the physical safeguards in place within the Human Resource Secretariat's (HRS) Pensions Administration and Group Insurance Division (Division). This Division administers the

public service pension and group insurance benefits. The mandate of the HRS, according to its 2014-15 Annual Report, is as follows:

> *The Human Resource Secretariat delivers human resource services by focusing on innovation, efficiency, clear standards, and consistent application of human resource policies across government. As noted earlier, the HRS also supports Treasury Board whose responsibilities are derived from the Financial Administration Act, the Public Service Collective Bargaining Act, and the Executive Council Act and Regulations.*

The Pensions Administration and Group Insurance Division was selected because of its close proximity to areas that are more open to visitors – the main lobby and the House of Assembly viewing gallery - and because of the potential for a large volume of personal information to be housed there. Access to the area by staff from other Divisions or Departments was also considered. The Department was notified of this Office's intent to audit on January 11, 2016 and the audit was conducted between January and May 2016.

Citizens expect the OIPC, as the oversight body, to assess the level of compliance with the law and best practice and to assist public bodies in establishing effective privacy management programs. Although there have been changes to the *ATIPPA* over the years and changing best practices, the standard for what is considered a reasonable physical safeguard has not really changed. It is expected that this will be one of the most mature areas to audit for *ATIPPA, 2015* compliance.

Audit Objectives

The objectives of this audit are to:

- establish considerations for physical safeguards that all public bodies can use when determining what is reasonable for the information in its custody or control;

- assess whether the Pensions Administration and Group Insurance Division has implemented adequate physical safeguards to protect the personal information in its custody or control;
- determine whether its policies, procedures and processes for safeguarding the information comply with the requirements of the *ATIPPA, 2015;*
- review the extent of staff compliance with the legislation, policies and procedures; and
- where appropriate, make recommendations to strengthen policy or practice.

The purpose of this report is to document, describe, comment and recommend improvements regarding the Division's physical safeguards, 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 focused exclusively on the physical safeguards in place at the Division, which is located on the main floor of the East Block of Confederation Building. In particular, the audit examined physical access to the Division by employees and guests (including members of the general public, stakeholders, government employees working in other locations, etc), the protection of personal information within the Division, and any associated policies and procedures. As an understanding of the personal information in the custody and control of the Division is necessary in determining if reasonable safeguards are in place, the audit also considered the information accessible by staff and stored on site.

Standards

This audit was conducted in accordance with the legislative mandate and practices of the Office of the Information and Privacy Commissioner of Newfoundland and Labrador, and is based on the standards recommended by the Canadian Institute of Chartered Accountants.

Audit Process

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 Canadian Institute of Chartered Accountants (CICA) as the standard against which audits will occur.

The audit started with background research information and a review of documents supplied by HRS. Once background information was reviewed, representatives from this Office conducted a site visit and administered a short survey to all Division staff. During the tour, OIPC representatives checked for evidence of physical safeguards and compliance with applicable policies and best practices.

Overview of Physical Safeguards

The *ATIPPA, 2015* requires that:

> *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.*

In general, a public body employs layers of technical, administrative and physical safeguards to ensure that it is in compliance with section 64.

What is considered reasonable?

Although this audit focused exclusively on physical safeguards, it is beneficial to examine Commissioner's Reports from this jurisdiction, as well as other Canadian jurisdictions, that discuss the criteria used to determine if safeguards are reasonable.

In Report P-2008-002, this Office identified four criteria it would consider when determining if reasonable safeguards were in place, including the foreseeability of the privacy breach, the seriousness of potential harm, the cost of preventative measures and the relevant standards of practice. While this Report was issued after a privacy breach, the same criteria could be used in a proactive fashion to better ensure a breach does not happen.

The Office of the Information and Privacy Commissioner of British Columbia noted in Investigation Report F12-02 that:

> *The measure of adequacy for these safeguards varies depending on the sensitivity of the personal information, the medium and format of the records, how the costs of security are estimated, the relationship between the public body and the affected individuals and how valuable the information might appear to someone intending to misuse it.*

British Columbia's Commissioner also noted, in Investigation Report F06-01, "The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances."

This is emphasized in the Office of the Chief Information Officer's (OCIO) *IP for IM Practitioners* (Information Protection for Information Management Practitioners) slide deck, which states, "security and safeguards should mirror information sensitivity and criticality." The OCIO's *Information Protection Guideline* promotes the protection of information through an understanding of the sensitivity and criticality of the information involved and placing reasonable safeguards that reflect the same.

Standards

It is important to examine the physical safeguard standards established by both the Government of Newfoundland and Labrador and the HRS in order to determine if appropriate safeguards are in place. The OCIO has developed a number of guidelines and best practices on a variety of topics, including many related to physical safeguards. While the guidelines can be adopted by anyone, they generally apply to public bodies as defined in the *Management of Information Act,* of which the Human Resource Secretariat is one.

It is important to note that not every reference to physical safeguards in government resources or HRS publications is mentioned below. Our review of documents, both those provided as part of the HRS submission and those obtained through our own research, revealed consistent messaging on physical safeguards, with many messages being repeated in a number of documents. This reflects best practice, as not all staff may read every document and, further, individuals need to hear messages multiple times. What follows is a summary of some of the best practices that have been identified.

General Physical Safeguards

General physical safeguards are discussed at a high level in a number of government documents, including the *Protection of Privacy Policy and Procedures Manual* produced by the Access to Information and Protection of Privacy (ATIPP) Office. Common physical safeguards include:

- locked filing cabinets, drawers and offices
- restricted access through the use of locks, swipe cards and security guards
- not leaving documents containing personal information on fax machines or printers
- using a cover sheet when faxing personal information
- secure disposal of records, such as shredding

The HRS prepared handout titled *Tips on How to Protect Personal Information* addressed many physical safeguards, including, but not limited to:

- *Know what records in your area contain personal information*
- *Lock up offices and filing cabinets and leave desks clean*
- *Limit access to personal information to only those who need it to do their job*
- *Lock your computer when you are away from your desk*

Fax Machines

The HRS prepared a handout called *Information Management (IM)* that included specific information regarding faxing personal information. It stated:

> *Think about information when you send a fax.*
>
> *When information is faxed there may be uncertainty as to who accesses it on the other end of the transmission. As a general rule, personal and/or confidential information should not be faxed. However, if it must be, then the following guidelines should be followed:*
>
> - *Avoid faxing confidential or personal information*
> - *Check fax numbers carefully*
> - *Use programmed numbers for frequently faxed locations*
> - *Notify the recipient that the fax is being sent*
> - *Verify with the recipient that the fax has been received*

The OCIO's document *FYI – Protecting Paper Records* further states that "if a fax machine is used to transmit or receive personal and/or confidential information, place it in a secure location whenever possible."

The ATIPP Office's *Protection of Privacy: Protecting Personal Information in the Workplace* recommends the use of cover sheets for faxes. It states, "…in the event that information is sent to an unintended recipient, the cover sheet will give instructions on how the disclosed information should be addressed or destroyed."

HRS encourages staff to consider alternate methods of transmitting personal information in the publication *Guideline for the Utilization of Encryption for Documents Containing Personal and Confidential Information*. It states:

> *If the situation permits, employees are encouraged to determine from the intended recipient if an encrypted email is possible. If that is not possible, inquiries about the security of the intended recipient's fax machine area should be considered. When sending faxes, employees are cautioned to take extra care in ensuring that the fax number is accurate.*

Printers

HRS' *Information Management* handout encourages, whenever possible, the use of a password if printing confidential or personal information on a device used by multiple staff and reminds staff to promptly pick up any print jobs.

Workspaces

The ATIPP Office's *Protection of Privacy: Protecting Personal Information in the Workplace* recommends adopting both a clean desk and a clean screen policy. The latter states, "Ensure that your computer is locked when leaving your desk for a short period of time and logged off if you are leaving for an extended period of time."

HRS' *Information Management* handout further instructs staff to lock their computers by pressing CTRL+ALT+DELETE on their keyboards if they are leaving their workstation and to clean their desks prior to departure at the end of the day.

The OCIO's *FYI – Password Management Best Practices* states, "do not share or write down passwords in any form such as taping to desk walls or terminals, storing in list finders and desk drawers, etc."

The OCIO's *FYI – Protecting Paper Records* states, "if you have to use a file cabinet in a public or shared areas of your office, ensure records are stored in a cabinet to which access can be limited to only those who have a requirement for access."

Outside the Office

The ATIPP Office's *Protection of Privacy: Protecting Personal Information in the Workplace* addresses working outside the office. It states, "If you must work from home or on the road, take a minimum amount of information needed to complete the assignment in order to avoid potential breaches. Each employee must ensure that the information is secure at all times."

The HRS prepared handout titled *Tips on How to Protect Personal Information* cautioned against removing personal information from the office, stating not to, "take personal information home with you unless it is necessary (if it is necessary for you to work at home, ensure that you follow the policies, guidelines, best practices outlined by the OCIO)."

The OCIO's *FYI – Information Protection: Safe Business Practices* states, "be careful when transporting information. Always double check that you do not leave information behind when exiting a car, room, etc. Don't carry loose documents or an open file folder."

With regards to transporting information, the HRS IM handout highlights best practices and reminds staff that human error is the cause of most security failures. It even highlights the need to avoid elevator conversations, where an informal conversation with a co-worker may lead to an unauthorized disclosure of information. This is reiterated in OCIO's *FYI – Information Protection: Safe Business Practices*, which states, "be discreet if you must view government information in public places."

The OCIO's presentation, *Recommended Approach to Encrypting GNL Files*, addresses the need to securely transport and store personal and/or confidential government information. It discusses the need to use encryption when storing or transporting information on a USB Flash Drive or a CD/DVD, among other issues.

OCIO's *FYI – Information Protection: Safe Business Practices* states, "A Virtual Private Network (VPN) connection and government issued laptop must be used to work on government information outside the office unless authorized by your Deputy Minister."

General Access

With regard to general access, the OCIO's *FYI – Information Protection: Safe Business Practices*, states, "If you have visitors to your work area for meetings, ensure that you follow your building security procedures to properly register their visit."

The OCIO's *FYI – Protecting Paper Records* states,"if you have a records storage area: restrict physical access, restrict access to keys, develop sign-out procedures for files, and segregate records and secure as appropriate any records which contain particularly sensitive information."

Physical Location

When it comes to physical location, best practice stems from the OCIO Guideline – *Physical Records Storage Development and Use*. This document states, in part, in the physical location and layout section:

- *Storage is best located in centre of a building. This mitigates many issues including:*
  - *Physical security components;*
  - *No windows for unauthorized entry;*
  - *Prevents UV damage to records;*
  - *Structural weight requirements due to the load of physical records on the floor.*
- *Avoid locations on the ground floor or in the basement of a building due to the risk of flooding;*
- *Protective coverings are recommended for open shelving to protect against damage in the event that the sprinkler system is activated, dust accumulation, etc.…*
- *A staging area used by staff to receive and process records. The size will be dependent on the anticipated volume of records and the number of staff.*
- *Consider the type of signage that will be used to identify the storage location:*

- *Hours of operation*
- *Emergency contact*
- *Directional signs that guide users from elevators, doors, etc.*

HRS Initiatives

In addition to the two handouts mentioned above, HRS has developed tools that all public bodies should consider adopting, if they do not already have something similar in place. In particular, it has established the Human Resource Secretariat Information Management (HRS IM) Committee and introduced both the *Divisional Checklist for Monitoring Protection of Personal Information* (*Divisional Checklist*) and the concept of teachable moments.

In 2015, the HRS IM Committee was created to increase information management and access to information and protection of privacy awareness, knowledge and skill within all HRS divisions. An IM and/or *ATIPPA* topic or issue is on each meeting agenda. Membership consists of a representative from each HRS division, including both the Group Insurance section and the Pensions Administration section of the Pensions Administration and Group Insurance Division, to serve as the IM/IP resource for the division. Many of the resources outlined above have been distributed and/or discussed at Committee meetings; in addition, many are centrally available to all staff in a folder on the shared drive called *IM Reference Material*.

This Committee introduced the *Divisional Checklist* to members. The *Divisional Checklist* was designed to identify areas where breaches could occur and try to mitigate the risk by making it a teachable moment for respective employees, where possible. The scope includes the physical workspace/areas of the Division.

The checklist process involved random checks of garbage, shredding and recycle bins; checking to see if items were left behind on printers and fax machines; ensuring the office and Registry were locked at the end of the day; overall workspace checks; and filing cabinet checks. It was indicated in the notes from the meeting that random privacy monitoring should occur at least once a month.

The Committee also established the concept of teachable moments, which highlights lessons learned from past breaches. These moments would discuss the breach and offer suggestions to avoid similar breaches in the future.

About the Division

The Pensions Registry is the central repository for plan member and administrative files required for the operation of the Pensions Administration Section, Pensions Administration and Group Insurance Division, Human Resource Secretariat. The Pensions Registry is divided into two sections; the main Registry and the vault. The Registry is located within the Pensions Administration section of the Division and contains active (pensioners) and pending (employee) pension records.

All information in the Group Insurance section is stored in locked filing cabinets, locked offices or in secured storage at the Mundy Pond Road site. An inventory of Group Insurance files is maintained in a spreadsheet.

When it comes to safeguards, a layered approach is often used, with physical, administrative and technical safeguards overlapping and complementing each other. The physical safeguards within the Division are also layered. For example, the Registry is a secure area within the secure Pensions Administration section, which is located in Confederation Building. Even prior to using an access card to enter the Division, an individual will have to be admitted by building security. At the entrance to the section is a reception desk that is occupied during regular business hours.

Just as access to the Division is controlled, so is the information that leaves the Division. Staff have access to either secure shredding bins or a shredder to ensure personal information is securely destroyed as per established retention schedules.

Improvements in physical safeguards for the Registry have been seen in recent years. In 2012, access to the Registry was not restricted, names and social insurance numbers (SIN) were featured on files and no inventory of records existed. In 2013, a registry file maintenance database was developed and registry procedures, such as the locked door

policy, were enforced. Today, new files do not feature the entire SIN and, although the older files still do, the restricted access to the Registry mitigates this risk.

The Registrar of Pensions also sought information regarding the Compensation and Benefits registry policy to ensure consistency with other government registries.

In September 2014, the Registrar of Pensions contacted the OCIO regarding physical security requirements for the protection of paper records. In response, the OCIO sent links to three publications: *Protecting Paper Records*, *Secure Storage and Disposal of Paper Records*, and *Physical Records Storage Development*.

Physical safeguards in the Registry are appropriate for the information stored within. The Registry is secured and access is restricted. Files are tracked using an electronic ticketing system and are only provided to authorized personnel for pension applications, medicals, deaths, survivor applications and pension adjustments. A process is in place to handle requests for member files from third parties. The removal of a file from the Vault follows the same process as file removal from the Registry. Once checked out, staff are responsible to ensure the Registry files remain secure at all time, such as storing them in a locked filing cabinet.

A full inventory of all plan member files, including their location, exists in the Registry Inventory System. Inventory is performed, on a rotating basis by last initial, by generating a printout of expected files from the system and then checking this listing against all files that are actually physically in the Registry.

Observations and Recommendations

Overall, all expected physical safeguards were identified during the audit process. While there are areas for improvement, some of which will be hampered by resource constraints, there were many examples of best practices in action. There was controlled access to the Division, further restricted access to the Registry and the Vault, and storage areas with locks, such as filing cabinets and desk drawers.

The staff survey demonstrated a solid awareness of physical safeguards and proactive, continuous improvements in safeguards have been documented.

Challenges include space constraints in the Registry and the Group Insurance section. The Registry has some active files stored in the Vault, as there is no room to accommodate them in the Registry, and the Group Insurance section is storing some files off-site in a secure facility. It must be noted that the Division is doing its best with the resources available.

Personal Information Collected/Personal Information Involved

The reasonableness of any safeguard ties directly back to the information involved. The public body collects personal information, some of which is sensitive, on both plan members and, in some cases, their dependents and spouses. As each file is unique and each will contain the minimum amount of personal information necessary for the identified purpose, the public body determined that all files should be protected to the highest standard. For example, all files within the Registry are tracked using a database and access to the Registry is restricted to authorized personnel.

Although the initial written submission from the Division did not include comprehensive documentation of the personal information housed within the Division, conversations with representatives demonstrated a comprehensive understanding of the types of information stored on site and the follow-up submission included a more detailed listing of the information fields.

During the course of the audit, prior to any formal recommendations from this Office, the Division developed a more robust description of the information collected by and stored in the Division. The Division developed an Excel spreadsheet listing data fields in the rows and the forms used for collection in the columns, providing a snapshot of the information collected, as well as the forms used for the collection.

In addition, the only information stored in an unlocked filing cabinet during the site visit was in a format that mitigated the risk as most individuals would not be able to read the information contained within.

Education and Awareness

Efforts have been made by HRS to promote information protection best practices, including physical safeguards, to all staff. In addition to promoting government resources, HRS has also produced several customized information protection publications. All HRS employees were directed to complete, among other courses, the ATIPP Online Training and the IM at Work Training. Although the HRS submission indicated that the training is mandatory and that completion is tracked by supervisors and directors, as of March 26th, not all staff had completed the courses. In addition, while these programs assist in building the foundation of understanding, there can be a disconnect between general training and job-specific application of the information learned.

The HRS IM Committee discussed a number of information protection topics and resource information was provided to members to communicate to their staff. Although emails were provided documenting that resources had been distributed to Committee members, Committee members did not consistently communicate the messages to staff.

While the results of the staff survey and the office tour demonstrated solid information protection best practices, there is little documentation that messages have been communicated to staff or that follow-up on mandatory training was conducted.

Accountabilities for training are defined. It is the responsibility of members of the HRS IM Committee to increase IM and *ATIPPA* awareness in their respective divisions. One of the roles of Directors is to ensure that employees are educated to their obligation to protect personal information.

Recommendation

> Develop a policy for information protection training and include responsibilities for training, follow-up on any mandatory training and consequences of non-compliance with the policy.

Public Body Response:

The Director for Pensions Administration and Group Insurance Division has worked with their division and the Centre for Learning and Development to ensure that the mandatory training requirement issued by the Deputy Minister in Sept. 2015 has been completed by all staff.

As previously reported, the Manager of Information Services, is developing a guideline document based on best practices that addresses the protection and security of both personal and confidential information. The purpose of this document is to ensure that the HRS meets its legal obligations under ATIPPA as well as the Management of Information Act. This document will be completed and submitted for Executive approval by September 30, 2016.

Recommendation

> Complementary training should be developed by the Division that links regular duties of employees with information protection best practices. This could be as simple as adding Information Protection as a standing agenda item for Divisional meetings. Even if there is no particular IP topic to discuss, this agenda item could be an opportunity for staff to ask questions.

Public Body Response:

Effective immediately all staff meetings will contain an "IM Minute" to deliver ad hoc IM training/tips for staff. In addition any relevant

information received from IM committee meetings will be disseminated to staff for further training and updates.

Accountability

The Director Responsible for IM and *ATIPPA* works to ensure that information on those topics is presented to senior managers and executives. Directors are accountable and responsible for ensuring that employees are educated regarding their obligations to protect personal information. Further, it is documented that it is the responsibility of members of the HRS IM Committee to increase IM and *ATIPPA* awareness in their respective divisions. The HRS submission also noted that it emphasizes that every employee has a responsibility under the *Management of Information Act* and the *ATIPPA, 2015*.

Recommendation

Document education and awareness activities during the year. While staff demonstrate best practice and high standards in information protection, there is little documentation on what activities contributed to this knowledge. Documenting training activities, even informal training activities, will assist in ensuring that all staff receive the messages being communicated and that the messages being communicated are consistent.

Public Body Response:

The Manager of IM Services has started a tracking worksheet for any training or information sessions presented or organized by the HRS IM resources. Both Pensions and Group insurance participate in IM month in April and various training communications throughout the year. Both sections currently have representatives on the HRS IM Committee and will begin documenting all training opportunities, activities, and detail what has been communicated.

Physical Space

Overall, the Division is in a good physical location and has appropriate physical safeguards in place. There are a number of challenges facing the Division, including space constraints, the presence of a sprinkler system in the Registry room and the lack of a dedicated fax line in the Group Insurance section. In particular, the sprinkler system in the Pensions Registry room could impact the ability of HRS to protect personal information against loss as required in section 64 of the *ATIPPA, 2015*.

Recommendation

While the Registry has a sprinkler system, the importance of these paper records warrant other fire suppression methods. The impact of the water damage would be major and could be the direct result of a malfunction. To mitigate this risk, it is recommended that HRS investigate suitable alternatives to a sprinkler system and make implementing a new system a priority. Please note that this recommendation applies only to the main Registry room that houses pension records.

Public Body Response:

The HRS recognizes the importance of the proper protection of paper files and the value of an appropriate fire suppression system. During Fiscal Year 2015-16, the HRS had intended to move the Division and associated records to another location which would have also addressed this matter. However, the move did not occur due to challenges experienced by the Department of Transportation & Works, as well as the pending establishment of the new Pensions Corporation. It is anticipated that the new Corporation may have plans to relocate in a consolidated space outside of the Confederation Building. As such, HRS will discuss this recommendation with the Corporation and include in transition planning.

Recommendation

> One of the long term recommendations from the pensions Registry inventory action plan from 2013 was the digitization of pension files. This would mitigate the risk that the paper files would be damaged or destroyed in a fire or sprinkler system malfunction situation and would save space. HRS should revisit this long term goal and develop a timeline for the project.

Public Body Response:

The HRS will apprise and discuss this matter with the new Pensions Corporation for the purposes of their future business.

Recommendation

> The Group Insurance section has been diligently working on scanning paper records into an electronic format. All current files have been placed in TRIM and work continues on getting historical files into TRIM as resources allow. As there are a large number of paper records in boxes in this section, as well as in storage off-site, HRS should revisit this project and identify the resources required to complete it.

Public Body Response:

The HRS recognizes the benefit that the use of TRIM has afforded the Group Insurance section and related work processes. Working within available financial resources and in the context of current work load demands, the HRS is endeavoring to continue this work. In the short term, a dedicated, temporary resource has been hired to focus on this activity during the next several months.

Recommendation

There is a door linking the Registry to an outside corridor. Although the corridor is located within a secure area, HRS should determine who has a key to the door. A policy should be developed regarding this door that requires the Registry Manager to check the status of the door on a regular basis to ensure it remains locked; should it ever be discovered unlocked, it should be reported to the ATIPP Coordinator and investigated appropriately.

Public Body Response:

The lock has been re-keyed and copies have been given to the Registrar and Manager, Pension Systems. Verification the door is locked has also been added to the HRS Privacy Monitoring Checklist.

Recommendation

It was suggested that the Registry may be moving out of its current location. This Office assumes that it will continue to be protected to the highest standard in any new location and during any move. The submission package from HRS provided details and best practice of a secure move. This Office expects any such move would be done in consultation with appropriate resources, including Information Management and the ATIPP Office, and that it would be done in a secure fashion. The recommendations contained in this report regarding the Registry, including restricted access and an alternative to the sprinkler system, would apply to any new location.

Public Body Response:

While it has not been confirmed that such a move will occur, the HRS anticipates that the new Pensions Corporation may be contemplating such a move. As such, the HRS will again apprise the Corporation of

these issues and recommendations as a part of transition planning and in its application of due diligence regarding the transfer of any information; physical or otherwise, to the Corporation.

Recommendation

The Group Insurance section has no fax machine in its office. While the fax machine is located in a secure area within HRS, it is shared with another Division. The Group Insurance section should obtain a dedicated fax line. This will also allow the Group Insurance section control over pre-programmed numbers, another safeguard that assists in the prevention of misdirected faxes.

Public Body Response:

The fax machine currently being used by the Insurance Division is located in the HRS Executive Office occupied by three (3) Assistant Deputy Ministers. A fax line has been requested for the Insurance Division and will be installed within the next month.

Policies, Processes, Procedures and Guidelines

Although the Pensions Administration section has the *Access to Information and Protection of Privacy Policy*, a number of instances of non-compliance were noted. However, staff were actually adhering to a higher standard than the policy required. For example, rather than picking up and returning files directly to the Registry, all file exchanges occur at the front reception desk, as it is constantly staffed and has a locked drawer for the files. This Office is hard pressed to fault a public body for non-compliance with policy when a higher standard is actually being practiced.

When first released, this policy was presented to staff in a meeting and a copy was sent via email. All policies are saved in a central location on a shared drive in a folder called *Policies, Procedures, Processes*.

No policies from the Group Insurance section were provided. Although not documented, the Group Insurance section demonstrated solid information protection practices during the tour and through the staff surveys. In addition, the risk of a policy gap is mitigated by the number of people in the section, as it is easier to ensure consistency with a small group operating in limited space.

Recommendation

> Group Insurance section develop policies regarding physical safeguards, as well as file retention/destruction.

Public Body Response:

The Insurance Division has been requested to draft this policy for Executive approval. It is anticipated that the policy wording will be completed by September 30, 2016. Preliminary work on file retention and destruction schedules has been started, however, it is anticipated a longer period of time will be required to obtain final approval due to the various steps in the approval process. The Insurance Division is developing a work plan and timelines to ensure the retention schedules are finalized as quickly as possible.

Recommendation

> Update the Pensions Administration section's *Access to Information and Protection of Privacy Policy* to reflect current practice.

Public Body Response:

An updated version of Pensions-001 – Access to Information and Protection of Privacy Policy has been forwarded to the Director of Pensions and Group Insurance for approval.

Recommendation:

> The HRS IM Committee recommended that *Divisional Checklists* be conducted monthly. The Division should develop documentation to address *Divisional Checklists*, including the process that should be followed when issues are identified. The Pensions -001-Access to Information and Protection of Privacy Policy already requires the Registrar, at least once a week, to conduct a spot check of staff working areas to ensure that files are being handled appropriately. HRS should develop a unified document that leverages best practices already in place.

Public Body Response:

The Pensions – 001 - Access to Information and Protection of Privacy Policy has been updated as of June 10, 2016 and now provides direction on the Divisional Checklist and Spot Checks.

Conclusion

Reasonable safeguards form part of a public body's duties to protect personal information as established in section 64 of the *ATIPPA, 2015*. The Government of Newfoundland and Labrador has established guidelines and standards to assist public bodies in identifying appropriate safeguards. During this audit, HRS demonstrated that it was aware of the government's resource material and had developed its own material to further complement the general guidelines.

If the Division is an indication of the physical safeguards in place throughout government, then this aspect of compliance with the *ATIPPA, 2015* is as mature as expected. While documentation was sometimes lacking and specific recommendations for improvement have been made, overall there were no major gaps in physical safeguards discovered during the audit. This Office encourages every public body to review the standards discussed in this report and conduct a review to determine its own level of compliance.

SIGNATURE PAGE

Title: Audit of Physical Safeguards

Public Body: Pensions Administration and Group Insurance Division
Human Resource Secretariat

Date: June 23, 2016

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