OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2018-002

March 14, 2018

Department of Fisheries and Land Resources

Summary: A technical error allowed some employees in the Department of Fisheries and Land Resources (FLR) to access, without authorization, files containing personal information of other employees. The Commissioner conducted an own motion investigation pursuant to section 73 of the *Access to Information and Protection of Privacy Act, 2015*. The Commissioner concluded that privacy breaches occurred, and that FLR failed to implement reasonable safeguards as required by section 64 of *ATIPPA, 2015*. While acknowledging FLR's efforts to date in responding to the breach, the Commissioner recommended additional measures.

Statutes Cited: *Access to Information and Protection of Privacy Act, 2015*, SNL 2015, c A-1.2.

Authorities Cited: Report PH-2016-001

File#: 0035-098-17-001

I BACKGROUND

[1] Many government departments maintain electronic records in shared folders with designated levels of permission to access specific folders. Some folders may be accessible to all employees of a department, while others might be accessible only to a department's executive. As the level of privacy of folder content increases, the number of employees with access should decrease correspondingly. If employees' duties do not require access to personal information, they should not have access to it.

[2] A department's obligations to safeguard the privacy of personal information are not limited to information provided by the public. Personal information provided by employees to employers, such as social insurance numbers, medical notes and employment history, should only be accessible to and used by staff in human resources or others who may require it to perform their duties.

[3] On October 26, 2017, the Department of Fisheries and Land Resources (FLR) learned from an employee in its Agriculture Business Development, Forest Ecosystem Management, Western Regional Services Division that she had accessed a folder containing personal information of a fellow employee. An audit of access to that folder determined that in the previous six months:

- 15 employees accessed 91 files in the folder without authorization; and,
- 3 of those 15 employees accessed the personal information of 10 different employees.

[4] FLR reported the privacy breach to this Office on November 8, 2017. FLR sought advice in regards to next steps, including the timing of notifying the impacted individuals. On first learning of the issue, FLR immediately moved to contain the breach by requesting that OCIO apply the restricted folder permission that ought to have been in place.

II PUBLIC BODY'S POSITION

[5] Permission to access the folder in question ought to have been limited to five FLR employees. Allowing access to all employees is contrary to the normal practices of the Office of the Chief Information Officer (OCIO) in assigning permissions to folders. OCIO opined that a technical issue led to a default permission (*Users*) to remain in place despite its efforts to assign restricted permission to access the folder in question.[1]

[6] FLR learned of the problem on October 26 when an employee advised a supervisor that she had access to a file containing the personal information of another FLR employee.

[7] As the result of an audit, FLR learned that the employee who reported the problem accessed six folders on October 26 and that each folder contained personal information of different FLR employees. On October 3, 2017, a second FLR employee appeared to have accessed a folder containing the personal information of another FLR employee. On September 7, 2017, a third FLR employee appeared to have accessed seven folders that contained the personal information of six different FLR employees. In all, 10 folders containing the personal information of FLR employees were accessed, without authorization, by accounts assigned to three of their co-workers. Personal information in some of these folders included social insurance numbers, banking information, medical information, dates of birth and driver license numbers of not only employees but also some of their family members.

[8] Staff from the Human Resource Secretariat (HRS) took the lead in investigating the conduct of the three employees. That investigation determined *that there was no intent on the part of the three individuals to have committed a privacy breach*. In fact, in regards to two of the three employees, it could not be determined that they accessed the personal information despite the audit tracing the activity to their network accounts.

[1] OCIO identified similar issues in two other departments and now conducts monthly audits across government to ensure appropriate permission levels are in place across government.

III DISCUSSION

[9] The scope of this breach, the sensitivity of some of the personal information and the length of time this vulnerability escaped notice led to our decision to commence an own motion investigation pursuant to section 73(3) of the *ATIPPA, 2015*. FLR received notice of the OIPC's own motion investigation on December 20, 2017.

[10] Section 64 requires that all public bodies take reasonable steps to ensure the protection of personal information from unauthorized access, use and disclosure. Those steps, often referred to as safeguards, include limiting access to personal information to only those required to have access to it to perform their duties. Safeguards require testing at the time of implementation and periodic review as part of a privacy management program in order to maintain their effectiveness.

[11] In this case, had an audit program existed, it would have discovered in a timely manner that all employees in FLR had access to files containing their co-worker's personal information. It is unknown for how long the folder in question was open to all FLR employees. It is also unknown, outside of the 6-month audit period, how many unauthorized accesses of these sensitive files occurred.

[12] OCIO advised FLR that it lacked the capacity to audit access to the folder beyond the previous 6-month period. That limitation severely limits the ability of public bodies and this Office to assess the extent of breaches and to hold to account those who have breached privacy.

[13] As noted, HRS conducted an internal investigation in regards to the three employees whose accounts accessed the files. In regards to the accesses on September 7 and October 3, those employees denied any knowledge of or involvement in accessing the files in question. One of them claimed that in his work area it was common practice to use terminals logged into and left open by coworkers. This practice results in the attribution of all activity on that terminal, including file accesses, to the account of the last person to have logged on to it using their unique network credentials. This practice fails to meet the

standards required by section 64 of the *Act*. It is a license to breach privacy with little, if any, risk of accountability.

[14] Our Report PH-2016-001 illustrates the mischief that stems from failing to implement and enforce timely log off protocols. In that instance, no one was accountable for a breach involving personal health information. Users should log off whenever they leave terminals unattended. It is essential that users log off terminals in common areas when leaving them. On the government network, if a user does not log off, twenty minutes elapse before the system times out and requires re-entry of a user's credentials. That is a significant window of opportunity for someone to commit a privacy breach under the guise of another user. The associated risks to privacy dwarf any inconvenience associated with logging back on to a vacated terminal.

[15] It is unclear from the HRS investigation whether and why the employee who reported the issue accessed the files of six employees. When she reported the issue to her manager, she advised that she had accessed a file containing the personal information of one employee. The audit revealed she had accessed the folders of six employees. Two sets of interview notes exist in association with her participation in the HRS investigation. One set attributes the other accesses to a request by the manager in the course of assessing the extent of the problem. The other set of notes record her lack of any recollection of accessing the other files.

[16] The manager focused on containment on learning of the breach. As such, the manager is unable to state whether she asked the employee to access any other files. The timing of the accesses as set out in the audit log is more consistent with the employee accessing all of the files prior to calling the manager; however, it is not possible to determine whether any of her accesses were intentional breaches of privacy.

[17] The two employees who denied accessing the files also took issue with the system being set up so they were able to access the personal information of their coworkers. This argument is valid, but only to a point. Mistakes happen, as occurred here. Inadvertently accessing personal information does not make an employee culpable. Continuing to

examine personal information, after recognizing it as something you should not have access to, is a willful breach of the *ATIPPA, 2015*. Employees cannot take money from an office petty cash drawer inadvertently left open. Similarly, they cannot knowingly access personal information simply because of an error allowing them to access a file.

[18] Unfortunately, at the time the three employees in question accessed the files containing their co-workers personal information, neither of them had received privacy training. This omission is particularly notable as one of them received discipline in the past for a privacy breach. A system of safeguards that omits regular and continuing privacy training fails to meet the standards set out in section 64 of the *Act*.

[19] As of January 29, 2018, 40 percent of FLR's executive and 30 percent of its staff has completed the online ATIPP training available to government employees via PSAccess. This 45-minute exercise should be a part of onboarding and required for completion on the first day of employment for all public body employees.

[20] Further, the online ATIPP training requires supplementation in the form of attending a session delivered by subject matter experts. The provincial ATIPP Office and the OIPC both offer to provide training at no cost to public bodies. Continuing education is also necessary to refresh the importance of privacy and update employees on current developments. It is the responsibility of managers, and ultimately the head of the public body, to ensure that the level of training provided is appropriate to the degree of sensitivity of information handled and the degree of access to that information provided to employees.

[21] Ultimately, a public body's privacy culture sets the tone in terms of the value placed on privacy. Culture flows downward. Managers who demonstrably prioritize privacy imbue employees with privacy values. Examples can be set in many ways, including discussing privacy at executive meetings and attending privacy training sessions with employees.

[22] A robust privacy culture, supplemented by employee training and reasonable safeguards, facilitates compliance with the *ATIPPA, 2015* and in so doing reduces the likelihood of privacy breaches.

IV CONCLUSION

[23] FLR is not unique in terms of the issues identified in this Report. Failures to restrict access, insufficient monitoring and inadequate training are common themes in the privacy complaints dealt with by this Office. The breaches here lead me to conclude that FLR failed to implement reasonable safeguards as required by section 64 of *ATIPPA, 2015*.

[24] While FLR failed to discharge its duty to implement reasonable measures to safeguard personal information against unauthorized access, there are many positive observations, including:

- FLR took immediate action to limit access to the folder in question;
- FLR notified this Office of the breach and sought advice regarding next steps;
- FLR notified impacted employees of the breach in a timely manner;
- FLR fully cooperated with our investigation, providing responsive records in a timely manner and promptly responding to further enquiries;
- FLR arranged in December of 2017 for the provincial ATIPP Office to provide privacy training to the staff in its Agriculture Business Development, Forest Ecosystem Management, Western Regional Services Division; and,
- FLR has committed to having all of its staff in all of its regions complete the PSAccess training by March 31, 2018.

V RECOMMENDATIONS

[25] As noted above, FLR took steps to limit access to the file in question to those requiring access in connection with their employment duties and commendably committed to all staff completing the PSAccess training. Under the authority of section 76(2) of the *ATIPPA, 2015*, I recommend that FLR take steps:

- To ensure that all staff complete the PSAccess training by March 31, 2018 and to provide this Office with confirmation of same;
- To develop a schedule for all staff to attend a privacy training session (personal or virtual), led by a subject matter expert, during fiscal year 2018-2019;

- To work with OCIO to attempt to suitably shorten default log off times;
- To routinely monitor for terminals left open and unattended and remind responsible employees of the requirement to log off; and,
- To develop policies addressing privacy training for new hires and for continuing privacy education for all staff with access to personal information.

[26] As set out in section 78(1)(b), the head of FLR must give written notice of his or her decision with respect to these recommendations to the Commissioner within 10 business days of receiving this Report.

[27] Dated at St. John's, in the Province of Newfoundland and Labrador, this 14th day of March, 2018.

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