OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2019-001

April 16, 2019

Royal Newfoundland Constabulary

Summary: An employee of the Royal Newfoundland Constabulary ("RNC") accessed a form containing the personal information of the Complainant (an RNC employee) and disclosed the personal information to other employees. The RNC acknowledged that this was a privacy breach of the Complainant's personal information. The Commissioner concluded that the Complainant's personal information was not properly protected under section 64 (protection of personal information) of the *Access to Information and Protection of Privacy Act, 2015* ("*ATIPPA, 2015*") and was improperly disclosed under section 68 (disclosure of personal information) of the *ATIPPA, 2015*. The Commissioner recommended that the RNC provide *ATIPPA, 2015* privacy training to the specific division of the RNC where the breach occurred. The Commissioner further recommended that the RNC communicate to all employees that personal information must be protected and only accessed and disclosed in accordance with the *ATIPPA, 2015*.

Statutes Cited: Access to Information and Protection of Privacy Act, 2015, SNL 2015, c A-1.2, sections 64 and 68.

Authorities Relied On: Royal Newfoundland Constabulary Policy and Procedure Manual on Confidentiality (General Order 339, October 27, 2015); Royal Newfoundland Constabulary Policy and Procedure Manual on Facilities (General Order 201, May 9, 2006); *Royal Newfoundland Constabulary Act, 1992*, SNL 1992, Chapter R-17; Royal Newfoundland Constabulary Regulations under the *Royal Newfoundland Constabulary Act, 1992* (O.C. 96-244).

File #: 0040-060-18-012

I BACKGROUND

[1] The Complainant submitted a privacy complaint to this Office alleging that the Royal Newfoundland Constabulary ("RNC") had not adequately protected her personal information, had improperly used her personal information and had improperly disclosed her personal information.

[2] In response to our investigation, the RNC explained that the Complainant had notified the RNC in July 2018 that she believed her personal information was breached as another employee had advised the Complainant that there was information about her being discussed within the RNC Division where the Complainant had worked (the "Division"). The Complainant alleged that someone had accessed her personal information contained on a form that was provided to her manager (the "Manager") regarding a workplace accommodation (the "Form"). The Form contained the Complainant's personal information, including medical information. The Complainant believed there was a breach as there was specific language used on that Form that would not have been known otherwise.

[3] The RNC conducted an internal investigation to determine if a breach had occurred. Members of the Division were either interviewed or given the opportunity to provide a written statement. Through the investigation an employee (the "Employee") of the Division admitted that she accessed and disclosed the Complainant's personal information contained on the Form. This Form had been located in the Manager's office. The Employee accessed the Form in the Manager's office, which was not locked, on a day that the Manager was not in the office.

[4] The RNC confirmed that the Complainant's personal information had been breached. The RNC determined that the Employee breached a number of provisions of the RNC's *Confidentiality Policy and Procedure Manual* (the "*Confidentiality Policy*"). The Employee was charged with two counts of conduct unbecoming a police officer for reading and disclosing the private information of the Complainant without consent and without the legal authority to do so. The Employee pled guilty to both counts and the Chief of Police imposed a sanction in February, 2019.

[5] The Complainant filed a privacy complaint with this Office in December 2018 as she had not received any update from the RNC regarding its internal investigation status since September 2018. The Complainant felt that a reasonable amount of time had elapsed for the RNC to complete its internal investigation and that she wanted a third party to follow up on her behalf. She also felt that the investigation had become less of a priority for the RNC as she was no longer an employee there.

[6] As informal resolution was unsuccessful, a formal investigation proceeded in accordance with section 74(2) of the *ATIPPA, 2015*.

II PUBLIC BODY'S POSITION

[7] The RNC confirmed that there was an inappropriate access and disclosure of the Complainant's personal information by the Employee and that it was a privacy breach. The RNC advised that the Employee called the Complainant to apologize for her actions.

[8] It was determined that the Employee was not compliant with the following sections of the RNC's *Confidentiality Policy*:

> *3.3 Employees shall not, without due authority, disclose in any manner, directly or indirectly to any person, any information or other matter that the employee may become aware of through the performance of her/his duties.*
>
> *3.4 Information that is to be kept confidential and private is information that would not otherwise be publicly available.*
>
> *a. Information that is to be kept confidential and private may be in any format, including (but not limited to) paper, electronic, film, visual or verbal disclosure which is created or received by the RNC in the course of its' service delivery.*
>
> *3.6 There are various categories of confidential information and private information, including, but not limited, to the following:*
>
> *…*

> *e. <u>Human Resources:</u>*
>
> *(1) Any and all personal and employment information that is gathered by the RNC.*
>
> *4.1 Individuals will be held accountable for breaches of confidentiality and/or privacy regarding RNC records or information. A breach includes intentional or unintentional unauthorized access to, use and/or disclosure in any manner (including written, electronic or verbal), directly or indirectly, of confidential or private information. A breach includes unauthorized access to recorded and/or unrecorded information including written, electronic and/or verbal information.*

[9] The RNC also determined that the Employee breached section 8(1)(g) of the *Royal Newfoundland Constabulary Act* which states:

> *8. (1) The duties of a police officer include*
>
> *…*
>
> *(g) obeying constabulary regulations, orders and rules respecting policy and procedures; and*
>
> *…*

[10] The RNC also found that the Employee breached section 7(1)(p) of the *Royal Newfoundland Constabulary Regulations* ("Regulations") which states:

> *7. (1) A police officer shall not*
>
> *…*
>
> *(p) engage in conduct unbecoming a police officer and liable to bring discredit upon the constabulary; and*
>
> *…*

[11] The Employee pled guilty to the two counts of conduct unbecoming a police officer and the Chief of Police imposed a sanction. The RNC also reported that the Manager's lack of physical security was addressed by the Manager's supervisor with respect to the RNC's policies on protection of information.

[12] During this investigation, specific questions were asked about how the RNC has dealt with this breach. In responding to those questions, the RNC provided very general

statements. The RNC was asked if there had been any steps taken to advise employees that accessing and disclosing other employees' personal information is not only a breach of the RNC's *Confidentiality Policy,* but also a breach of the *ATIPPA, 2015*. The RNC responded that it has sent out communication regarding confidentiality and that it will continue to inform employees during routine notices.

[13] In this breach there was a number of weeks that elapsed from when the Employee accessed the Complainant's personal information and disclosed it to other employees and when the breach was reported to the RNC. The breach was only reported when another employee eventually told the Complainant there was information about her being discussed. When asked about whether a reminder had been sent to employees of their responsibility to report a breach, the RNC's response was that RNC employees have completed mandatory ATIPP training as well as Fostering a Harassment Free Workplace 2018 training.

[14] When asked if the RNC has taken any steps to prevent further breaches of this kind or advise employees that they must keep personal information secure, the RNC responded advising that it has an IM/IT Policy and that employees will be reminded of this policy again in a routine manner, as well as during Information Management week. When asked about physical security, the RNC responded that it has secure areas designated under its Facilities Policy, and that employees will be reminded of these secure areas.

[15] When asked about training, the RNC advised that it was open to having specific *ATIPPA, 2015* privacy training provided to the Division.

III COMPLAINANT'S POSITION

[16] The Complainant advised that she felt her personal information was not protected, and was improperly accessed and disclosed without her consent. The Complainant advised she was seeking change at the RNC and wanted the person responsible to be held accountable.

[17] The Complainant advised that she sought an accommodation and that she was very concerned about her privacy. She was assured by Human Resources that her privacy would be a top priority and that the only people who would have knowledge of her file would be her Manager and Human Resources.

[18] While the Complainant resigned from the RNC for another employment opportunity, she stated that her decision to resign was a direct result of the uncomfortable, unsupportive, shaming and hostile work environment that she experienced since the breach of her privacy.

[19] The Complainant expressed her desire for transparency and accountability within the RNC. She feels that this privacy breach and the subsequent poor treatment she was subjected to are indicative of the workplace culture within the RNC and how accommodations are handled and viewed. The Complainant feels that individuals at the RNC will continually be afraid to seek accommodations or help if the result is a breach of privacy and poor treatment.

[20] The Complainant stated that she felt this breach was malicious and that this type of a breach is representative of a systemic issue relating to the workplace culture within the RNC. She feels that the attitude of many officers is that they are entitled to know information because of who they are.

[21] The Complainant feels that the RNC has inadequate policies and practices surrounding the privacy of its members and that there must be stronger policies and practices in place to protect employees. She stated that the lack of physical security in the Manager's office demonstrated that controls were not in place even after the breach was reported.

[22] The Complainant expressed dissatisfaction with the length of time it took the RNC to investigate the breach and expressed concern with the organization investigating itself.

IV DECISION

[23] Sections 64(1)(a) and 68 of *ATIPPA, 2015* are as follows:

> *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;*
>
> *...*
>
> *68. (1) A public body may disclose personal information only*
>
> *...*
>
> > *(c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose as described in section 69 ;*
> >
> > *....*
>
> *(2) The disclosure of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.*

[24] It is clear that the Complainant's personal information was accessed and disclosed in contravention of sections 64(1)(a) and 68 of the *ATIPPA, 2015*. This occurred as a result of the Employee accessing and disclosing the Complainant's personal information without consent and without authority under the *ATIPPA, 2015*.

[25] The RNC Inspector noted at the end of the internal investigation that the Employee had made several comments which were concerning as there appeared to be a lack of understanding or concern about the privacy of others.

[26] The RNC investigation revealed that the Manager often left his door open and unlocked when he was not in the office. The Employee claimed the Form was on the Manager's desk when she viewed it, however, the Form was located by the Inspector assigned to the investigation in the Manager's desk drawer. The comment was made by the investigating Inspector that the Form was not located easily.

[27] While there was a dispute over the location of the Form as there had been a time lapse between the Employee accessing the information and the Inspector locating the Form in the Manager's desk, it was still accessed improperly by the Employee and the contents disclosed improperly by the Employee.

[28] I have serious concerns regarding the lapse in physical security practices in this case. The RNC has a *Facilities Policy and Procedure* ("*Facilities Policy")* which states:

> *9. Office Security*
> *All offices, rooms, or other facilities occupied by employees of the RNC shall be locked at all times when unoccupied or not in use.*

[29] Employees should lock their offices when not in use, however, it was reported that the Manager would leave his office unlocked when he was not in the office. Other employees reported they would sometimes drop off paperwork to his office. While the RNC advised that the Manager's supervisor has addressed this issue with the Manager, I must stress that the RNC risks further privacy breaches by not ensuring that employees follow its own office security policy and I strongly recommend further and targeted communication with all employees on this issue.

[30] Also the RNC *Confidentiality Policy* has a section which speaks to the duty to protect confidential and/or private information. Section 8 of the *Confidentiality Policy* states:

> *8.0 Duty to Protect Confidential and/or Private Information*
>
> *8.1 RNC employees owe a positive duty to:*
>
> a. *Protect the confidentiality of the information that is in her/his custody. or under her/his control, or within her/his knowledge, and the privacy of any individual who is the subject of that information.*
>
> b. *To comply with the requirements of all applicable legislation, which includes the Access to Information and Protection of Privacy Act, regarding personal information and the privacy of individuals who are the subject of that information.*
>
> c. *To provide for the secure storage retention and disposal of personal information and confidential information and to minimize the risk of*

> *unauthorized access to or disclosure of the personal information of individuals or confidential information.*
>
> *d. To comply with the reasonable requirements of the RNC which may include, but are not limited to that s/he identify the purpose of the use or access to personal information contained in RNC records.*

[31] The RNC has policies in place regarding the protection of personal information. The RNC must remind employees of these policies on a regular basis and not just in a "routine manner". Furthermore, senior management must demonstrate and communicate their support for these policies.

[32] While the RNC advised it was open to having specific *ATIPPA, 2015* privacy training provided to the Division, the RNC must also educate and remind employees about the privacy provisions in the RNC's own *Confidentiality Policy* and the *ATIPPA, 2015*. A breach is an opportunity for a public body to review its policies and procedures, educate employees and take steps to ensure future breaches do not occur in the same manner.

[33] This breach may have been prevented if the Manager had followed the RNC's physical security protocols by locking his office door. This obligation extends to all employees who have a responsibility to protect personal information. Additional measures that provide protection include locking desk drawers and filing cabinets.

[34] This Office has already provided two training sessions on *ATIPPA, 2015* privacy to members of the Division. We note that it is the continuing responsibility of the RNC to ensure that its employees follow the law. Without education, training and an environment that respects personal information, more breaches can be expected, and RNC leadership will be held accountable.

[35] Also of note, the RNC did not file a privacy breach notification with this Office in a timely manner. The breach was reported to the RNC in July 2018 by the complainant. The RNC received notice of the Complaint to the OIPC on December 17, 2018. The RNC did not send the breach notification form to the OIPC until January 10, 2019. Reporting privacy breaches to the OIPC is mandatory under section 64(4)

> *(4) Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.*

[36] In our guidance on filing a privacy breach, we request that public bodies do so "immediately once you become aware of a privacy breach". We recognize that there may be some time lag in reporting, in particular when confirmation of the breach is required, but six months is far too long.

VI RECOMMENDATIONS

[37] Under authority of 76(2) of the *ATIPPA, 2015*, I recommend that the RNC:

1. Ensure that its practices are consistent with its policies and procedures by communicating to all employees the importance of complying with the RNC *Confidentiality Policy* and the *ATIPPA, 2015* regarding reporting privacy breaches as well as only accessing and disclosing personal information, (including other employees' personal information), in accordance the *ATIPPA, 2015*;

2. Ensure that the requirement for physical security measures is communicated to all employees and enforced. These include locking offices, computers, desk drawers, filing cabinets, etc. that house personal information; and

3. Remind employees on a consistent basis that there are RNC policies regarding confidentiality and physical security as well as a legal requirement under the *ATIPPA, 2015* to protect privacy.

[38] As set out in section 78(1)(b) of the *ATIPPA, 2015*, the head of the RNC must give written notice of his or her decision with respect to these recommendations to the Commissioner and any person who was sent a copy of this Report (in this case, the Complainant) within 10 business days of receiving this Report.

[39] Dated at St. John's, in the Province of Newfoundland and Labrador, this 16th day of April 2019.

Victoria Woodworth-Lynas
Information and Privacy Commissioner
Newfoundland and Labrador (A)