Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 322-2017, 120-2018

Saskatchewan Legal Aid Commission, Ministry of Corrections and Policing

May 3, 2019

Summary: Saskatchewan Legal Aid Commission (Legal Aid) proactively reported a privacy breach. It reported that an employee of the Ministry of Corrections and Policing (the Ministry) disclosed the personal information of an individual to a Legal Aid Employee. The Commissioner found that the disclosure was not authorized by *The Freedom of Information and Protection of Privacy Act* (FOIP) and that the Ministry did not respond appropriately to the breach. He recommended that the Ministry investigate further and amend its *Code of Professional Conduct*. He also recommended that Legal Aid continue to improve its privacy training for employees.

I BACKGROUND

[1] On December 6, 2017, Saskatchewan Legal Aid Commission (Legal Aid) proactively reported a privacy breach to my office. An employee of Legal Aid (LA Employee) was provided information about an individual in custody (the affected individual) at Saskatoon Correctional Centre (SCC) from a SCC employee (SCC Employee). SCC is operated by the Ministry of Corrections and Policing (the Ministry).

[2] The affected individual was arrested by the Saskatoon Police Service (SPS) in September 2017 and was placed in custody at SCC. It is my understanding that it is a regular practice of SPS to place individuals in custody in cells at SCC during busy periods such as long weekends.

[3] This disclosure of information was discovered by Legal Aid on November 24, 2017, during an internal investigation into another matter. The affected individual was known to the LA Employee. Legal Aid advised that it was informed by the LA Employee that a SCC employee disclosed the affected individual's name, the fact that the individual was in custody and the related charges. The LA Employee's lawyer also indicated to my office verbally on September 20, 2018 that the SCC employee provided other information that was personal in nature and offered an opinion about the affected individual.

[4] As a practice, SPS routinely disclosed information about individuals in custody to Legal Aid so that the individuals have an opportunity to access services from Legal Aid. I discussed this process in Investigation Report 121-2018 and 122-2018. However, the disclosure in question occurred outside of the established routine procedure between SPS and Legal Aid. Further, this established procedure does not disclose all of the specific data elements that were disclosed to the LA Employee.

[5] My office notified Legal Aid that we would be conducting an investigation on December 13, 2017. However, Legal Aid's investigation was hampered by the LA Employee's unwillingness to cooperate and provide information about the disclosure and the SCC employee who made the disclosure. On July 4, 2018, my office also notified the Ministry that my office was investigating.

[6] In this case, the LA Employee refused to cooperate with Legal Aid's investigation. The LA Employee also refused to cooperate when my office contacted them directly. Finally, after suggesting that I conduct an interview under oath, the LA Employee stopped communicating with their lawyer and my office has been unable to contact them directly.

[7] Because of the LA Employee's unwillingness to cooperate, Legal Aid, the Ministry and my office have not been able to establish specific details of this breach such as the detail of the charges disclosed, the time and date of the disclosure, the method of the disclosure or the identity of the SCC employee who disclosed the information. However, the LA Employee's lawyer confirmed they received the personal information in question from an employee of SCC.

[8] My office shared a copy of this Draft Report with Legal Aid and the Ministry. In response, the Ministry indicated that a "disclosure of personal information within the Ministry was never confirmed." It also noted that the way in which it "approached the file was largely dictated by the fact that there was insufficient evidence to determine that a disclosure had occurred". My approach in this investigation is to acknowledge Legal Aid's report that an SCC employee disclosed personal information to the LA Employee. This was substantiated by the LA Employee's lawyer. As such, I will conclude that there was a disclosure of personal information.

II DISCUSSION OF THE ISSUES

1. Does *The Freedom of Information and Protection of Privacy Act* apply in these circumstances?

[9] The privacy provisions of *The Freedom of Information and Protection of Privacy Act* (FOIP) apply when three elements are present. The first element is a government institution, the second element is personal information, and the third element is if the personal information is in the possession or control of the government institution.

[10] The Ministry qualifies as a government institution pursuant to subsection 2(1)(d)(i) of FOIP. Legal Aid is prescribed as a government institution in *The Freedom of Information and Protection of Privacy Regulations* in Part I of the Appendix. As such, it is considered a government institution pursuant to subsection 2(1)(d)(ii) of FOIP.

[11] As noted earlier, the SCC employee disclosed the affected individual's name, related charges, other information that was personal in nature and offered an opinion about the affected individual. Personal information is defined in subsection 24(1) of FOIP. The relevant provisions are as follows:

> 24(1) Subject to subsections (1.1) and (2), "personal information" means personal information about an identifiable individual that is recorded in any form, and includes:
>
> …
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> …
>
> (h) the views or opinions of another individual with respect to the individual;
>
> …
>
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
>
> (ii) the disclosure of the name itself would reveal personal information about the individual.

[12] The charges laid against the affected individual qualify as personal information pursuant to subsection 24(1)(b) of FOIP. The opinion about the affected individual qualifies as the affected individual's personal information pursuant to subsection 24(1)(h) of FOIP. The affected individual's name appears with other personal information. Therefore, it qualifies as personal information pursuant to subsection 24(1)(k)(ii) of FOIP.

[13] Further, the items listed in subsection 24(1) of FOIP is not meant to be exhaustive. There can be other types of information that would qualify as personal information that are not listed. Part of that consideration involves assessing if the information has both of the following:

1. Is there an identifiable individual?
2. Is the information personal in nature?

[14] The affected individual is identifiable to the LA Employee and Legal Aid. Personal in nature means that the information reveals something personal about the individual. The other information about the affected individual that was personal in nature would qualify as personal information pursuant to subsection 24(1) of FOIP.

[15] The information is in the possession or control of the Ministry.

[16] I find that FOIP applies.

2. Was disclosure of the personal information in question authorized by FOIP?

[17] Both Legal Aid and the LA Employee's lawyer have suggested that the disclosure of personal information was authorized by subsection 29(2)(m) of FOIP, which provides:

> 28(2) Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed:
>
> …
>
> (m) where necessary to protect the mental or physical health or safety of any individual;

[18] However, it is up to the government institution that first had possession or control to decide what information is disclosed and under what authority; in this case, the Ministry. Further, the Ministry should have a protocol in place to make decisions about disclosures that are not routine, such as disclosures made in accordance with subsection 28(2)(m) of FOIP. Government institutions should be clear about the authority to disclose before a disclosure is made.

[19] In the investigation report that the Ministry provided to my office, it did not indicate that it relied on subsection 28(2)(m) of FOIP to disclose the personal information in question.

[20] The Ministry provided me with its *Disclosure of Information* policy from its *Adult or Youth Policy Manual.* The following excerpts are relevant to this discussion:

> **4.0 <u>Offender Personal Information</u>**
>
> 4.1 Offender file documentation and information may be disclosed without the offender's consent for the specific purposes established in Section 29(2) of *FOIP* including, but not exclusive to:
>
> …
>
> 4.1.7. Where necessary, to protect the mental or physical health or safety of any individual;
>
> …
>
> 4.2 Within the framework of the preceding conditions, the facility director or regional director or designate may disclose offender file information without consent in the following situations:
>
> 4.2.1. To authorized representatives of any municipal, provincial or federal government criminal justice agency (police, courts, other correctional systems);
>
> 4.2.2. To representatives of government ministries (Social Services, Health, etc.) and to non-government organizations (John Howard Society, Mobile Crisis Centre, etc.) if these departments and organizations are currently providing a direct service to the offender and/or there is reason to believe the release of this information will assist the offender in developing and maintaining responsible and rehabilitative behavior.
>
> …

[21] This policy states at paragraph 2.1 that the "Executive Directors of Corrections are accountable for all information released by correctional staff, and therefore must have general knowledge and/or control of what is being released." However, the Ministry indicated that the Executive Director does not authorize the disclosure of personal information in every instance. I must stress that Executive Directors should ensure that any disclosure of personal information that is not routine should be carefully examined through a privacy lens. In this instance, the Ministry indicated that the Director of the SCC had no knowledge of the disclosure of personal information in this particular case.

[22] As such, I must conclude that the disclosure of the affected individual's personal information was not authorized by FOIP.

3. Did the Ministry respond appropriately to this privacy breach?

[23] In order to be satisfied, my office needs to be confident that the Ministry took the privacy breach seriously and took all necessary steps. In multiple resources, my office recommends five best practice steps be taken by a government institution when responding to privacy breaches. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Plan for prevention; and
5. Write a privacy breach report.

[24] In this case, I will use these steps to assess the Ministry's response to the breach.

[25] I acknowledge that this breach has been a challenge to investigate given the limited information that has been provided. However, in the investigation report that the Ministry submitted to my office, it indicated that it has insufficient information to determine that a privacy breach has occurred despite the assertions of Legal Aid and confirmation from the LA Employee's lawyer.

Contain the breach

[26] Upon learning that a privacy breach has or may have occurred, government institutions should immediately take steps to confirm and contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; or
- Correcting weaknesses in physical security.

[27] The Ministry was informed of the incident 10 months after the incident allegedly occurred. It conducted an investigation based on the limited information. I am satisfied that the Ministry took steps to contain the breach as much as possible at that late date.

Notify affected individuals

[28] Notifying an individual that their personal information has been inappropriately accessed or disclosed is important for a number of reasons. Not only do individuals have a right to know, they need to know in order to protect themselves from any potential harm that may result from the inappropriate disclosure. Unless there is a compelling reason not to, government institutions should always notify affected individuals.

[29] In this case, there is some sensitivity in this matter that I cannot discuss in this public report. Because I do not have as much information as I would like and for other reasons, I do not recommend that the Ministry inform the affected individual at this time.

Investigate the Breach

[30] Once the breach has been contained and appropriate notification has occurred, the government institution should conduct an internal investigation. The investigation is generally conducted by the government institution's access and privacy unit because they have the appropriate privacy expertise to do so and understand what the relevant privacy legislation requires of their organization. The investigation should address the incident on a systemic basis and should include a root cause analysis. It should also consider whether the safeguards that were in place at the time of the incident were adequate. The investigation should be documented in an internal privacy breach investigation report. At the conclusion of its investigation, the government institution should have a solid grasp on what occurred.

[31] The Ministry indicated that its investigation involved consulting directly with Legal Aid. It also discussed the matter with the Director of the SCC. Finally, it reviewed the safeguards.

[32] With respect to safeguards, the Ministry discussed the following administrative safeguards in its investigation report.

[33] As previously noted in this report, the Ministry has a policy regarding the disclosure of personal information about those in custody to members of the public. It also indicated that decisions about such disclosures are to be made by the Director of the facility. The Director of the SCC did not authorize the disclosure in question.

[34] The Ministry advised that all Corrections staff complete the Saskatchewan Government's Access and Privacy self-directed learning module. It also advised that all new Corrections Officers complete the Induction Training Program, which includes a module facilitated by the Access & Privacy Branch. This module includes best practices for dealing with privacy and security concerns within a correctional facility.

[35] The Ministry also referred to the *Code of Professional Conduct* that employees sign annually and *Oath or Declaration of Office*. In Investigation Report 319-2017, I commented on these documents and recommended that the Ministry amend its *Code of Professional Conduct* to include more explicit and specific language about the protection of personal information and personal health information. The Ministry indicated at that time that it would take this recommendation under advisement the next time they update the document. I again make this recommendation.

[36] My office also suggested during the course of this investigation that it check the emails and telephone records of its employees during the time the affected individual was in custody. The purpose would be to see if there were any disclosures of personal information to the LA Employee. It declined to do so as there were between 100-200 employees on staff each of day the affected individual was in custody and it would be a very time and resource intensive process. It again noted that it concluded that there was insufficient evidence to confirm that a breach of privacy has occurred.

[37] I disagree with the Ministry's conclusion that there is insufficient evidence to conclude that a privacy breach occurred. Both Legal Aid and the LA Employee's lawyer indicated that an SCC employee disclosed this personal information.

[38] The Ministry has suggested that the term "corrections employee" will sometimes be used incorrectly if people are not familiar with the corrections environment. Employees working for the courts, police service, etc. may be misidentified as a corrections employee. The LA Employee has worked for Legal Aid for a number of years and would have been familiar with the environment.

[39] The Ministry also indicated that Legal Aid suggested that the LA Employee may have obtained the information in question by reading the affected individual's disclosure report. Legal Aid's privacy breach report indicated that a non-staff lawyer handled the affected individual's case. As a result, the report stated that Legal Aid did not request or receive the disclosure report.

[40] The Ministry also indicates the information about the privacy breach that it has received has been unreliable. The LA Employee has not indicated who provided the information and has informed Legal Aid that they do not recall how the information was shared. Again, I accept that investigating the breach under these circumstances has been challenging. However, lack of further information does not make the information that has been received untrue. The LA Employee's allegation that an SCC employee disclosed personal information merits investigation.

[41] I am not satisfied that the Ministry thoroughly investigated the breach. I recommend that it investigate this matter further, which would include searching telephone and email records.

Plan for prevention

[42] The next step is to formulate a plan to avoid future breaches of a similar nature. Some changes that are needed may have revealed themselves to the government institution during the investigation phase, such as deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training. This is an important step in addressing a privacy breach because a privacy breach cannot be undone but the government institution can learn from it and improve.

[43] The Ministry did not list any plans for improvement.

Write a privacy breach report

[44] The Ministry provided my office with a privacy breach report.

4. Did Legal Aid respond appropriately to this privacy breach?

[45] I will use the same steps to assess Legal Aid's response to the breach.

Contain the breach

[46] In this case, the LA Employee collected the personal information from the SCC employee. The personal information collected was similar to personal information that it would have collected about the affected individual by Legal Aid from SPS, but the collection came through inappropriate channels.

[47] When Legal Aid found out about the breach a few months after it allegedly occurred, Legal Aid investigated and proactively reported it to my office.

Notify Affected Individuals

[48] As discussed earlier in the report, there is no need to notify the affected individual.

[49] Also, I acknowledge that Legal Aid had difficulties getting information from the LA Employee. However, it should have notified the Ministry after learning of the breach.

Investigate the Breach

[50] The method that Legal Aid took to investigate the breach included interviewing the LA Employee. However, as noted, the employee was uncooperative.

[51] Legal Aid searched the email accounts and telephone records associated with the LA Employee. Legal Aid was unable to determine which employee of SCC disclosed the information.

[52] Legal Aid indicated that it viewed the incident as gossip. Legal Aid also suggested the disclosure may have been made pursuant to subsection 29(2)(m) of FOIP.

[53] Regardless if it was an intentional disclosure or gossip, the personal information was in the possession and control of both the Ministry and Legal Aid; both government institutions. FOIP applies to this personal information. Authority must exist at the time of the disclosure for it to be appropriate. Employees of government institutions must understand how to collect, use and disclose personal information in accordance with FOIP. Section 24.1 of FOIP provides:

> 24.1 Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:

> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[54] Legal Aid also looked into privacy related training that its employee had received at Legal Aid. It indicated that there was a privacy in-service in 2015. However, Legal Aid did not take attendance and it cannot confirm if this employee had attended.

[55] In Investigation Report 226-2017, I noted that Legal Aid accepted my recommendation in my office's draft report that it implement a program of mandatory annual training for all employees. I issued the report after the alleged incident. Legal Aid has indicated that it has developed an online training module for all employees to complete annually. It is in the process of ensuring all of its employees have completed the training. It is also keeping a record to ensure all employees successfully complete the module. I recommend Legal Aid keep working towards this.

[56] Further, my office asked Legal Aid if the LA Employee had also signed an annual confidentiality agreement. It indicated that employees sign a letter of offer which has a clause about confidentiality. The LA Employee signed one several years ago.

[57] Upon review, the clause in the letter of offer does not mention FOIP. Further, Legal Aid is also subject to *The Health Information Protection Act* (HIPA). This is not addressed in the letter of offer. I recommend that Legal Aid require its employees to sign annual confidentiality agreements with specific language about FOIP and HIPA.

Plan for prevention

[58] With respect to prevention, Legal Aid indicated that one of its managers reviewed the expectation of confidentiality with the LA Employee.

Write a privacy breach report

[59] Legal Aid provided my office with a privacy breach report.

III FINDINGS

[60] I find the disclosure of personal information was not authorized by FOIP.

[61] I find the Ministry did not respond appropriately to the breach.

IV RECOMMENDATIONS

[62] I recommend that the Ministry amend its *Code of Professional Conduct* to include more explicit and specific language about the protection of personal information and personal health information.

[63] I recommend that the Ministry investigate this matter further, which would include searching telephone and email records.

[64] I recommend that Legal Aid continue its work in implementing a program of mandatory annual training for all employees.

[65] I recommend that Legal Aid require its employees to sign annual confidentiality agreements.

Dated at Regina, in the Province of Saskatchewan, this 3rd day of May, 2019.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner