Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 200-2018

Saskatchewan Legal Aid Commission

November 27, 2019

Summary: Saskatchewan Legal Aid Commission (SLAC) proactively reported a privacy breach after discovering the office doors to its Melfort office were mistakenly left open overnight. The Commissioner found that SLAC did not have appropriate safeguards to protect personal information and personal health information when the incident occurred and that SLAC did not take appropriate steps to prevent future privacy breaches. The Commissioner recommended SLAC develop and implement a policy or procedure for identifying affected individuals and considerations to determine if notice is necessary. The Commissioner also recommended SLAC develop and implement appropriate safeguards to protect personal information and personal health information.

I BACKGROUND

[1] On September 24, 2018, Saskatchewan Legal Aid Commission (SLAC) proactively reported a privacy breach to my office:

> On Thursday, September 20th, one of our staff lawyers [lawyer A] arrived at our office in Melfort and found both entrance doors unlocked and wide open.
> …
>
> The Legal Director and the other staff lawyer [lawyer B] left the office at 5:15 p.m. on September 19th. Both doors were locked. [Lawyer A] arrived at 4:59 a.m. on September 20th. Both doors were open.
>
> The Building Manager for Central Services checked the building records and confirmed that no one entered the building overnight until our lawyer arrived at 4:59 a.m.

> [The Building Manager] confirmed that the cleaning crew was in our office at 10 p.m. on September 19th. Lastly, [they] confirmed that the construction crews were not present that evening (the floor was recently renovated and the crew is completing the last tasks after hours).
>
> The Cleaning Supervisor has spoken to the cleaners and they understand the seriousness of this incident. The Cleaners are external contractors.
>
> No materials within the office were disturbed and nothing appears to be missing.

[2] On September 27, 2018, my office requested SLAC provide an internal investigation report, details of the breach and copies of relevant documents, such as written policies, procedures or agreements.

[3] On October 12, 2018, SLAC provided my office with its internal investigation report.

II DISCUSSION OF THE ISSUES

1. Is *The Freedom of Information and Protection of Privacy Act* (FOIP) or *The Health Information Protection Act* (HIPA) engaged and do I have authority to investigate this matter?

[4] SLAC 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 qualifies as a government institution pursuant to subsection 2(1)(d)(ii) of FOIP. SLAC is also considered a trustee pursuant to subsection 2(t)(i) of HIPA.

[5] Subsection 24(1) of FOIP and subsection 2(m) of HIPA provide:

> **Section 24(1) of FOIP**
>
> **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:
>
> > (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;

(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;

(c) **Repealed.** 1999, c.H-0.021, s.66.

(d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;

(e) the home or business address, home or business telephone number or fingerprints of the individual;

(f) the personal opinions or views of the individual except where they are about another individual;

(g) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual;

(h) the views or opinions of another individual with respect to the individual;

(i) information that was obtained on a tax return or gathered for the purpose of collecting a tax;

(j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or

(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.

Subsection 2(m) of HIPA

2 In this Act:

…

(m) **"personal health information"** means, with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;

(ii) information with respect to any health service provided to the individual;

(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information;

[6] SLAC advised my office that its records were not stored in locked cabinets or locked offices at the end of the day. Therefore, when the cleaning staff accessed the space to perform their services and mistakenly left the doors to the SLAC Melfort office propped open, all of the records stored at that location that contained personal information and personal health information would be involved in this incident. While SLAC has indicated that it did not appear that any of the records were accessed, SLAC would have to conduct a complete audit to verify no records were missing. Additionally, SLAC did not take steps to secure records in locked cabinets or locked offices when they were aware cleaning staff would be entering after hours.

[7] In Investigation Report 299-2017 involving SLAC, my office investigated a privacy breach involving a missing client file and found that personal information was involved and FOIP applied. In Investigation Report 231-2017 and 317-2017 involving SLAC, my office investigated a privacy breach incident involving a disclosure file and found that it contained both personal information and personal health information and both FOIP and HIPA were engaged. In Investigation Report 226-2017 involving SLAC, my office investigated a privacy breach incident involving a stolen DVD containing a victim's impact statement and also found that this contained personal information and personal health information; therefore, both FOIP and HIPA were engaged.

[8] These are just a few examples of the types of personal information and personal health information that would be held by SLAC; therefore, I find the records at issue would

include both personal information and personal health information and both FOIP and HIPA would be engaged.

[9] I find that both FOIP and HIPA apply and subsections 33(d) of FOIP and 52(d) of HIPA provide my authority to investigate this matter.

2. Did SLAC respond appropriately to the privacy breach?

[10] In order to be satisfied that the breach has been appropriately responded to, my office needs to be confident that SLAC took the privacy breach seriously and took all necessary steps when learning of it in a timely manner. In multiple resources and reports, my office recommends a public body/trustee respond to a privacy breach by considering five best practice steps. These steps are:

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

[11] I will use these steps to assess SLAC's response to the incident.

Contain the breach

[12] 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 was breached.
- Revoking access to personal information or personal health information.
- Correcting weaknesses in physical security.

[13] As noted earlier, on the evening of September 19th, the SLAC employees indicated that the doors were closed and locked when they left for the day. The morning of September 20th, the SLAC lawyer arrived at the Melfort Office and found the doors had been left propped open. Upon this discovery, the SLAC lawyer closed the doors to secure the office and prevent any further unauthorized access to the information by anyone who entered the building.

[14] However, SLAC has failed to cease its practice of leaving personal information and personal health information on desk surfaces and storing this information in filing cabinets and offices that do not have the ability to lock when cleaning staff are accessing the office. SLAC must ensure that it properly safeguards personal information and personal health information.

[15] Need-to-know is the principle that personal information or personal health information should only be available to those employees in an organization that have a legitimate need-to-know of that information for the purpose of delivering their mandated services.

[16] The cleaning staff's services do not require access to SLAC's records and they do not have a need-to-know the personal information or personal health information contained in SLAC's records.

[17] SLAC indicated the Cleaning Supervisor spoke to the cleaning staff of the importance of closing the office doors after completing their duties. However, SLAC's practices of allowing cleaning staff to have access to the office when records are not properly safeguarded has not ceased. Therefore, every occasion that cleaning staff enter the SLAC office when records are not safeguarded results in another breach of privacy.

[18] SLAC's has not appropriately contained the privacy breach, as its practice does not properly safeguard personal information or personal health information from unauthorized access by individuals that do not have a need-to-know.

Notify affected individual(s) and/or appropriate organizations

[19] Notifying an individual that their personal information or personal health 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.

[20] SLAC noted in their investigation report that it is unknown how many individuals are affected, as it did not appear that any records in the office had been disturbed and there was no evidence anyone had entered the building between the hours the office doors were left open. However, as no records were properly secured, the personal information and personal health information of any individuals files stored in that office could have been inappropriately accessed by anyone in the building.

[21] Section 29.1 of FOIP provides the following regarding notifying an individual of unauthorized use or disclosure of personal information:

> **29.1** A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[22] SLAC did notify my office of the breach of privacy incident, but it does not appear SLAC took into consideration the need to notify any affected individuals. In the future, SLAC should take additional steps to identify affected individuals and to determine if notification is necessary.

[23] I recommend SLAC develop and implement a policy or procedure for identifying affected individuals when a breach occurs and defining considerations for SLAC when determining whether or not notice to affected individuals is necessary.

Investigate the breach

[24] 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.

[25] SLAC's internal investigation report provided:

> The Melfort Office is in the Provincial Government Building… It shares a floor with the Ministry of Health. The building is locked between 5:00 p.m. and 7:00 a.m. After hours access requires a FOB which is only issued to building employees. The Legal Aid office has an external locked door that opens into a reception area. There is a second locked door between the reception area and the offices… The cleaning crew was in our office at 10 p.m.… No materials within the office were disturbed and nothing appears to be missing.

[26] My office followed up with SLAC asking for additional information regarding what safeguards SLAC has in place to ensure only those with a need-to-know can access records and prevent unauthorized access to personal information and/or personal health information, and requested copies of any relevant policies or procedures. SLAC provided the following:

> There are a number of practices and barriers in place.
>
> 1. Members of the public cannot leave the reception area of our Area Offices.
>
>   Any non-staff member cannot leave the reception area without a staff member. In many of our offices, including Melfort, there is a locked door between the reception area and the rest of the office. In other offices, there is a half-wall with a finger lock on it. In those offices, the reception area opens into a "bullpen" of admin staff.

One admin staff is expected to remain within the bullpen anytime that the front door is unlocked.

2. Staff members escort members of the public within the secured area.

   When a member of the public enters the secured area of the office, they are escorted by a staff member the entire time that they are within the secured area. If they are meeting with a lawyer, the lawyer will meet them at reception, be with them during the meeting and then walk them out.

3. Janitorial staff are encouraged to clean during the day. All janitorial staff are bonded.

   As we use government buildings for our offices, we have limited control over the scheduling and qualifications of the cleaning staff. However, we have requested that Central Services have our staff clean during the day if at all possible. As well, all cleaning staff are bonded.

4. Storage of electronic records.

   Our IT policy sets the expectation that everyone locks their computer when they leave the room. If left unattended, our computers lock after 30 minutes of inactivity. As well, our client database automatically logs out after 15 minutes of inactivity.

5. Storage of paper records.

   We encourage all paper records to be stored in filing cabinets, banker's boxes, briefcases and file rooms. This practice is encouraged and not required due to the confines of our physical space in some area offices.

[27] Section 24.1 of FOIP establishes the government institution's duty to protect personal information:

> **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.

[28] HIPA contains a similar provision for the duty to protect personal health information at section 16:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the information;
>
> (ii) loss of the information; or
>
> (iii) unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[29] SLAC also stated that the lawyer's office doors and filing cabinets do not have the ability to lock; therefore, none of SLAC's records were stored in locked cabinets or locked offices when SLAC staff left the office. My office asked if SLAC was willing to implement a clean desk policy or practice in an effort to informally resolve this matter, but SLAC advised it felt it was not possible to implement due to the volume of records and how records are stored.

[30] SLAC does have a *Client Information Management Policy* that provides the following about the protection of client information:

> 1. In the office
>
> Protecting client information while in the office is as important as protecting client information outside of the office. Common sense measures can and should be taken to reduce risks to personal information in such situations.

> 1.1 When in the office,
>
> i. Client files shall not be left in public areas.
>
> ii. Members of the public, including clients, shall be escorted when in private areas including offices and hallway.
>
> iii. Information on other clients shall not be visible when meeting with clients in an office.
>
> iv. [SLAC] encourages employees to adopt a clean desk policy when possible. Under a clean desk policy, employees would tidy desk of papers and files with personal information in them at the end of each work day. **Papers and files would be locked in filing cabinets or desk lockers overnight.**
>
> [Emphasis added]

[31] I am glad to see that SLAC has a policy encouraging a clean desk policy; however, when SLAC is aware that external parties, such as cleaning staff, will be entering their offices after hours, storing records containing personal information and personal health information in locked cabinets or locked offices should be required. SLAC also noted in this policy that information on other clients should not be visible when meeting with clients. However, this section of the policy should apply to anyone that does not have a need-to-know, including external parties entering the SLAC office.

[32] Ensuring the most basic physical safeguarding of records containing personal information or personal health information has been discussed in past reports. In Investigation Report LA-2013-003 involving a school division, the former Commissioner stated:

> [81] Physical safeguards for Student B's personal information could have included a locked filing cabinet for each faculty member assigned to a certain case load of students. The file cabinets should also be in a room that is either constantly supervised or which has a lock on the door. These physical safeguards would need to be described in written policies and procedures.
>
> [82] Administrative safeguards, also described in written policies and procedures, would cover, among other things, the following:
>
> - That all personal information should be kept within the cabinets at all times unless it is in use by authorized individuals. Individuals authorized to use the personal information should be clarified;

> - Personal information should not be lying around on a desk in a room where students or staff without a need-to-know frequent;
>
> - When file cabinets and rooms should be locked and who should have access;
>
> - Personal information is subject to access to information requests and should be in a filing system where it is easily retrievable if required to do so; and
>
> - The training programs to make employees aware of these policies and procedures as well as LA FOIP in general. I will discuss this in more detail below.

[33] In Investigation Report 205-2015 involving a doctor, my office found that:

> [8] During my investigation, Dr. Bartsch indicated that neither her house nor her briefcase was locked. These are basic physical safeguards that were not in place. Dr. Bartsch also provided my office with the privacy policy of her office. The privacy policy does not address physical safeguards to protect personal health information… This is an essential administrative safeguard which was not in place. This lack of safeguards did not protect against a reasonably anticipated threat to the security or integrity of the information. Dr. Bartsch did not meet the duty to protect as outlined in section 16 of HIPA.

[34] While it is my office's expectation that any public body or trustee have appropriate safeguards in place to protect personal information or personal health information, those in the legal profession also have a responsibility to safeguard personal information and personal health information. The Office of the Privacy Commissioner of Canada's resource *A Privacy Handbook for Lawyers PIPEDA and Your Practice*, provides the following guidance to lawyers regarding the obligation to safeguard personal information:

> Safeguarding Personal Information
>
> Lawyers are familiar with the need to safeguard their clients' information…
>
> Lawyers can face a number of potential vulnerabilities in the course of their practice, including the following:
>
> - Poor security measures for paper documents, computer systems, computer applications, mobile devices, computer networks, wireless networks or email transmission;
> - Misplacing paper or electronic documents;
>
> …

> PIPEDA requires personal information to be safeguarded at all times. Personal information should be safeguarded through the use of:
>
> - Physical measures, for example, locked filing cabinets and restricted access to offices;
> - Organizational measures, for example, security clearances and limiting access on a "need-to-know" basis;
>
> …
>
> The more sensitive the information is, the stronger the safeguards must be…

[35] The Law Society of Saskatchewan's *Code of Professional Conduct* provides the following regarding a lawyer's obligation to safeguard a client's information:

> **3.5 Preservation of Clients' Property**
>
> Preservation of Client's Property
>
> In this rule, **"property"** includes a client's money, securities as defined in The Legal Profession Act, 1990, original documents such as wills, title deeds, minute books, licences, certificates and the like, and all other papers such as client's correspondence, files, reports, invoices and other such documents, as well as personal property including precious and semi-precious metals, jewelry and the like.
>
> **3.5-1** A lawyer must:
>
> (a) care for a client's property as a careful and prudent owner would when dealing with like property; and
>
> (b) observe all relevant rules and law about the preservation of a client's property entrusted to a lawyer.
>
> Commentary
>
> [1] The duties concerning safekeeping, preserving, and accounting for clients' monies and other property are set out in the Rules of the Law Society of Saskatchewan.
>
> [2] These duties are closely related to those regarding confidential information. **A lawyer is responsible for maintaining the safety and confidentiality of the files of the client in the possession of the lawyer and should take all reasonable steps to ensure the privacy and safekeeping of a client's confidential information. A lawyer should keep the client's papers and other property out of sight as well as out of reach of those not entitled to see them.**
>
> [Emphasis added]

[36] Finally, SLAC has taken the position that because cleaning staff are bondable, there should not be an issue with them being in an office where personal information and personal health information are not properly safeguarded.

[37] Whether or not cleaning staff are bonded, they do not have any need-to-know personal information or personal health information and therefore should not have ready access to it. SLAC has an obligation to protect personal information and personal health information but its current practices do not go far enough to meet these obligations pursuant to sections 24.1 of FOIP and 16 of HIPA.

[38] SLAC concluded that the cause of the incident was that cleaning staff left the office doors open. However, SLAC is the government institution/trustee that has the obligation to ensure personal information and personal health information is properly safeguarded, not the cleaning staff.

[39] I find that SLAC did not have appropriate safeguards in place to protect personal information and personal health information at the time of the privacy breach incident.

Plan for prevention

[40] 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.

[41] The only preventative step identified by SLAC was the Cleaning Supervisor discussed the incident with the cleaning staff and assured them it would not happen again. While it is an important reminder for cleaning staff, SLAC should have also evaluated the safeguards it had in place at the time of the breach to determine if improvements could be made to prevent future occurrences.

[42] SLAC's safeguards and its practice of allowing cleaning staff to enter the office after hours when records are not properly safeguarded fails to protect records that contain personal information and personal health information, as required by sections 24.1 of FOIP and 16 of HIPA. This practice results in a privacy breach each time that someone without a need-to-know accesses the office as records containing personal information and personal health information are not secured.

[43] I find that SLAC has not implemented appropriate safeguards to prevent future breaches of privacy.

[44] I recommend SLAC develop and implement appropriate safeguards to protect personal information and personal health information, as required by sections 24.1 of FOIP and 16 of HIPA. This should include the use of physical safeguards, such as storing records containing personal information and personal health information in offices with locked doors or locked filing cabinets to prevent unauthorized access to these records. As well as, amendments to its administrative safeguards as outlined in paragraph [31].

Write a privacy breach report

[45] SLAC provided my office with a privacy breach report that contained the necessary elements.

III FINDINGS

[46] I find that both FOIP and HIPA are engaged.

[47] I find that SLAC did not have appropriate safeguards in place to protect personal information and personal health information at the time of the privacy breach incident.

[48] I find that SLAC has not implemented appropriate safeguards to prevent future breaches of privacy.

IV RECOMMENDATIONS

[49] I recommend SLAC develop and implement a policy or procedure for identifying affected individuals when a breach occurs and defining considerations for SLAC when determining whether or not notice to affected individuals is necessary.

[1] I recommend SLAC develop and implement appropriate safeguards to protect personal information and personal health information, as required by sections 24.1 of FOIP and 16 of HIPA. This should include the use of physical safeguards, such as storing records containing personal information and personal health information in offices with locked doors or locked filing cabinets to prevent unauthorized access to these records. As well as, amendments to its administrative safeguards as outlined in paragraph [31].

Dated at Regina, in the Province of Saskatchewan, this 27th day of November, 2019.

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