Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 231-2017 & 317-2017

Ministry of Justice and Saskatchewan Legal Aid Commission

March 8, 2018

Summary: While attending court, an accused individual decided to represent himself, rather than having a Saskatchewan Legal Aid Commission (SLAC) lawyer represent him. While court was in session, the SLAC lawyer returned what he thought was the accused disclosure file to the prosecutor who then passed the file to the accused. The following day, the accused contacted the Ministry of Justice (Justice), Public Prosecutions office and my office to advise that he had received someone else's disclosure file. The Information and Privacy Commissioner recommended both Justice and SLAC notify the affected individuals of the breach of privacy and develop written policies or procedures for handling disclosure files.

I BACKGROUND

[1] On September 18, 2017, a concerned individual (Individual A) contacted my office advising that he had received a disclosure file that was not his, from the Ministry of Justice (Justice), Public Prosecutions (Prosecutions) office.

[2] Based on my office's conversation with Individual A, he had contacted Prosecutions to advise of this error and was instructed to return the file to their office. Individual A also stated that a lawyer with Saskatchewan Legal Aid Commission (SLAC) advised him he should return it to Prosecutions.

[3] Individual A contacted my office to report the incident and agreed to provide my office with a copy of the record via registered mail and return the original copy to Prosecutions.

[4] On September 20, 2017, my office notified Justice that it would be initiating a privacy breach investigation and requested a copy of its internal investigation report and copies of any relevant policies and/or procedures.

[5] After receiving a copy of Justice's internal investigation report, my office noted that this privacy breach incident also involved SLAC. On December 6, 2017, my office provided SLAC with notification that my office had initiated a privacy breach investigation regarding this matter. My office requested a copy of SLAC's internal investigation report regarding the incident and copies of any relevant policies and/or procedures.

II DISCUSSION OF THE ISSUES

[6] Justice is considered a government institution pursuant to subsection 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP). Justice is also considered a trustee pursuant to subsection 2(t)(i) of *The Health Information Protection Act* (HIPA).

[7] 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 is considered 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.

1. Does FOIP and/or HIPA apply in these circumstances?

[8] The disclosure file received by Individual A includes a cover page originating from Justice's Prosecutions office to SLAC providing documents by way of disclosure. This cover page includes the name of the accused (Individual B) and the name of another individual that provided statements in relation to the domestic violence occurrence. The file includes two police officers' reports of the domestic violence occurrence, the two individual's statements, Individual B's criminal record and a report listing Individual B's convictions and non-convictions.

[9] The information in this file includes information that would qualify as personal information pursuant to subsection 24(1) of FOIP, such as address, date of birth, criminal history, etc. The file also includes information regarding injuries sustained as a result of the domestic violence occurrence which would qualify as personal health information pursuant to subsection 2(m) of HIPA.

[10] I find that both FOIP and HIPA apply.

[11] Although not formally addressed in its internal privacy breach report submitted to my office, during a telephone conversation with my office Justice did question whether subsection 2(2)(c) of FOIP would have any application to this incident as the disclosure file was provided to Individual A while court was in session.

[12] Subsection 2(2)(c) of FOIP provides as follows:

> **2**(2) **"Government institution"** does not include:
> …
>
> (c) the Court of Appeal, Her Majesty's Court of Queen's Bench for Saskatchewan or the Provincial Court of Saskatchewan.

[13] In both Justice and SLAC's internal investigation reports, it provides that Individual A advised the prosecutor during his appearance in Regina Domestic Violence Court (DVC) that he would be representing himself on his charges going forward. While DVC was in session, a lawyer with SLAC returned the disclosure file to the prosecutor. The prosecutor then handed the disclosure file to Individual A. Based on both parties internal investigation reports, it does not appear that either the prosecutor or the SLAC lawyer confirmed Individual A's identity matched that of the disclosure file. Upon reviewing the disclosure file, Individual A found that it was Individual B's file. The following day Individual A notified Justice's Prosecutions office advising he had received the incorrect file.

[14] From my understanding, the records in question are not those of the courts, but appear to be records that originated from Justice's Prosecutions office and provided to SLAC through

the disclosure process. Further, the records were not disclosed to Individual A by the courts, rather through a transaction that involved both Justice and SLAC.

[15] Both Justice and SLAC have a duty to appropriately safeguard personal health information in its possession or control pursuant to section 16 of HIPA. As well, prior to January 1, 2018, my office's position was that government institutions had an implied duty to protect personal information under FOIP. As of January 1, 2018, the duty has now ben enshrined in statute at section 24.1 of FOIP. This section imposes a duty upon government institutions to protect personal information in its possession or control.

[16] As such, I do not find that subsection 2(2)(c) of FOIP applies to this incident.

2. Did Justice and SLAC respond appropriately to the privacy breach?

[17] When there is a privacy breach, my office's focus is determining whether the public body has appropriately handled the privacy breach. My office's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities* (Privacy Breach Guidelines), recommends trustees take the following five steps when responding to a privacy breach:

- Contain the breach;
- Notify affected individual(s);
- Investigate the breach;
- Prevent future breaches; and
- Write a privacy breach report.

Contain the breach

[18] My office's Privacy Breach Guidelines provide the following regarding containing the breach:

> It is important to contain the breach immediately. In other words, ensure that personal information is no longer at risk. This may involve:
>
> - Stopping the unauthorized practice.
> - Recovering the records.
> - Shutting down the system that was breached.

- Revoking access to personal information.
- Correcting weaknesses in physical security.

[19] As noted earlier in this report, the SLAC lawyer intended to return Individual A's disclosure file to the prosecutor but instead handed him Individual B's disclosure file. The prosecutor then handed Individual B's disclosure file to Individual A.

[20] After discussions with the Prosecutions office, the lawyer from SLAC, and my office, Individual A provided my office with a copy of the record and gave the original back to the Prosecutions office.

[21] Therefore, I find that this breach of privacy was adequately contained.

Notify affected individual(s)

[22] The SLAC lawyer advised he had contacted Individual B to notify him that his disclosure file had unintentionally been provided to Individual A. Justice indicated in its internal investigation report that the prosecutor notified the SLAC lawyer so that he could notify his client.

[23] In reviewing the record, there appears to be two affected individuals. There does not appear to be any attempt to provide notification to the second individual identified in this file by either SLAC or Justice. Further, it is not clear what details the SLAC lawyer included when he contacted Individual B. In my office's Privacy Breach Guidelines, it provided the following details should be included when providing notification to affected individual(s):

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g. name, credit card numbers, medical records, financial information, etc.).
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g. how to contact credit reporting agencies, how to change a health services number or driver's license number, etc.).
- Contact information of an individual within your organization who can answer questions and provide further information.

- A notice that individuals have a right to complain to the IPC. Provide contact information.
- Recognition of the impacts of the breach on affected individuals and an apology.

[24] As both Justice and SLAC had the opportunity to verify disclosure file was Individual A's before providing it to him and both have obligations under FOIP and HIPA to protect personal information and personal health information in their possession or control, both parties share the obligation to notify the affected individuals.

[25] I recommend that both SLAC and Justice provide notification to both of the affected individuals providing the details as set out in paragraph [23].

Investigate the breach

[26] The Privacy Breach Guidelines provides a list of key questions to ask during a breach investigation. These questions include:

- When and how did your organization learn of the privacy breach?
- What occurred?
- How did the privacy breach occur?
- What is the applicable legislation and what specific sections are engaged?
- What safeguards policies and procedures were in place at the time of the privacy breach?
- Who are the affected individuals?

[27] Both SLAC and Justice's internal investigation reports appear to agree on the facts as to how Individual A ended up with Individual B's disclosure file. Individual A's account of how he ended up with Individual B's disclosure file also appears to match the information found in both parties investigation reports. As such, I find that SLAC and Justice have appropriately investigated this privacy breach.

Prevent future breaches

[28] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. The public body should ask themselves the question, what steps can be taken to prevent a similar privacy breach?

[29] In its internal investigation report, Justice provided the following regarding its procedure for handling DVC disclosure files:

> The Public Prosecutions Division of the Ministry of Justice does have a standard internal procedure for handing out DVC disclosure packages in DVC. The DVC prosecutor, when interacting with a self-represented individual, will provide him/her with a set of instructions on how to obtain a disclosure from their office. The individual must contact the Domestic Violence administrative assistant directly for the disclosure. The disclosure must be picked up by the individual from the Public Prosecutions office located in Regina and will only be released to individuals with valid photo identification… At the same time, the prosecutor retains a discretion to provide disclosure directly to an individual in DVC, but that is to happen only when the person is established on the DVC record to be the accused or is otherwise known to the prosecutor as the accused, and upon the prosecutor verifying the correct material is being provided to the accused.

[30] In order to prevent a similar privacy breach from occurring in the future, Justice indicated that prosecutors would no longer provide disclosure files to the accused while DVC was in session on busy days, unless certain circumstances existed that it was required to do so.

[31] My office followed up with Justice requesting a copy of its internal written standard procedure for handling disclosure files. However, Justice indicated that there was no written internal policies or procedures. My office also requested Justice clarify what it considered to be a "busy day" in court and what exceptions may apply for not following its formal procedure. Justice indicated that on the day in question the SLAC lawyer was handling a heavier caseload than usual, this would have been considered a "busy day" in court. Further, Justice indicated that there are circumstances in which a judge may order the prosecutor to provide the disclosure file to the accused while court is in session, this would be one exception to the standard procedure.

[32] SLAC's internal investigation report regarding preventative measures summarizes its understanding of Justice's change in process regarding disclosure files released including that defence counsel would no longer be able to return the disclosure file to the prosecutor while court was in session. Beyond that, SLAC indicated it did not anticipate any additional changes in process for SLAC.

[33] I recommend that Justice document its standard procedure for handling disclosure files in an internal policy or procedure. The policy or procedure should detail the two ways that a disclosure file can be provided to the accused; either through their formal process by attending the Prosecutions office or during court where the judge orders the prosecutor to do so. The policy and/or procedure should detail how the identity of the accused will be verified before providing the disclosure file and how the exchange will be documented to ensure there is a record that the information was provided to the accused and when it was provided.

[34] I recommend SLAC also develop and implement a policy or procedure of the steps that will be taken when returning a disclosure file to Prosecutors. The policy and/or procedure should include details about when it is appropriate to return disclosure files, steps to ensure the accurate disclosure file is returned to Prosecutions and how it will document when the file is received from Prosecution and when it has been returned.

Write a privacy breach report

[35] Documenting the privacy breach and the organization's investigation into the matter is a method to ensure that the organization follows through with plans to prevent similar privacy breaches in the future.

[36] Both Justice and SLAC documented its investigation into the privacy breach in a report that was submitted to my office. I find that the trustee has fulfilled this step of responding to a privacy breach.

IV FINDINGS

[37] I find both FOIP and HIPA apply to this incident.

[38] I find that the privacy breach has been adequately contained.

[39] I find both Justice and SLAC have obligations under FOIP and HIPA to notify the affected individuals.

[40] I find that the privacy breach was adequately investigated.

[41] I find both Justice and SLAC require written policies and/or procedure for handling disclosure files to prevent future breaches from occurring.

V RECOMMENDATIONS

[42] I recommend both SLAC and Justice provide written notification to the affected individuals, ensuring the letter includes the details outlined at paragraph [23] of this report.

[43] I recommend Justice document its standard procedure in an internal policy or procedure for handling disclosure files and verifying identity of the accused as outlined at paragraph [33] of this report.

[44] I recommend SLAC develop an internal policy or procedure for handling disclosure files as outlined at paragraph [34]

Dated at Regina, in the Province of Saskatchewan, this 8th day of March, 2018.

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