



INVESTIGATION REPORT 226-2017

Saskatchewan Legal Aid Commission

October 23, 2017

Summary: Saskatchewan Legal Aid Commission (SLAC) notified the Information and Privacy Commissioner (IPC) of the theft of a laptop that contained a DVD with personal information/personal health information. The IPC found that SLAC responded appropriately to the privacy breach. The IPC recommended that SLAC ensure all mobile devices and storage devices transported outside of the office are properly encrypted and password protected and kept with the employee at all times in a locked briefcase.

I BACKGROUND

- [1] On September 1, 2017, a Saskatchewan Legal Aid Commission (SLAC) Lawyer transported a work laptop from Regina to Wynyard.
- [2] On September 4, 2017, the Lawyer discovered the work laptop, containing a victim statement on a DVD, was missing from his work vehicle.
- [3] On September 11, 2017, SLAC proactively reported the privacy breach to my office.
- [4] On September 25, 2017, SLAC provided my office with its internal investigation report.

II DISCUSSION OF THE ISSUES

1. ***Does The Freedom of Information and Protection of Privacy Act (FOIP) and/or The Health Information Protection Act (HIPA) apply in these circumstances?***

- [5] The DVD with the victim's statement was provided to SLAC' Lawyer through disclosure. As the DVD was not recovered, SLAC could not provide details regarding the information contained in the victim's statement. However, SLAC advised the video statement of the victim provided her full name and statement of the sexual assault she was victim to and likely included her medical information.
- [6] The Legal Aid Saskatchewan website provides "The Saskatchewan Legal Aid Commission is a governance board responsible for ensuring that the strategies, goals, policies, and directions of the organizations are implemented through delegation to the Legal Aid Saskatchewan management."
- [7] SLAC is prescribed as a "government institution" in *The Freedom of Information and Protection of Privacy Regulations* in Part I of the Appendix.
- [8] SLAC would also be considered a "trustee" as defined by subsection 2(t)(i) of HIPA.
- [9] Subsection 24(1) of FOIP and subsection 2(m) of HIPA provide definitions of personal information and personal health information respectively.
- [10] Based on the nature of the victim's video statement, it is safe to assume that both personal information and personal health information are involved.
- [11] I find that both FOIP and HIPA apply.

2. Was the privacy breach responded to appropriately?

- [12] My office's resource *Privacy Breach Guidelines for Government Institutions and Local Authority* recommends the following five steps for responding to a breach of privacy:
- Contain the breach,
 - Notification,
 - Investigate the breach,
 - Prevent future breaches, and

- Privacy breach report.

[13] I will consider each of these steps to determine if the privacy breach was responded to appropriately.

Contain the breach

[14] The first step in responding to a privacy breach is containing the breach, which means to stop the unauthorized practice when the trustee learns of it.

[15] When SLAC learned the laptop containing the DVD with the victim's statement was missing, it contacted Wynyard RCMP, the Crown Prosecutor on the file, and requested court clerks in Wynyard look for the laptop, specifically in the interview rooms. Unfortunately, the laptop and DVD have not been located.

[16] I find that SLAC has made reasonable efforts to contain the breach.

Notification

[17] My office recommends that notification contain the following elements:

- A description of the breach (a general description of what happened).
- A detailed description of the personal health information involved (e.g. name, medical records, etc.).
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advise on actions the individuals can take to further mitigate the risk of harm and protect themselves (e.g. how to change a health services number).
- 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 my office. Provide contact information.
- Recognition of the impacts of the breach on affected individuals and an apology.

- [18] On September 25, 2017, SLAC provided a letter to the affected individual advising that a laptop containing a DVD with one of her statements had been stolen. It also advised that the DVD had not been found and that Wynyard RCMP had been notified of the theft.
- [19] The letter also contained contact information of representatives from SLAC and my office.
- [20] While SLAC did advise the affected individual that the stolen disc contained her statement, it was not clear that it was a video statement. It is possible the victim provided more than one statement regarding this matter and is not aware if it was a written, audio or video statement. In my office's draft report, I recommended SLAC notify the affected individual that the disc contained a video statement provided by her to ensure she is fully informed of this incident.
- [21] SLAC responded to this recommendation advising it had contacted the Crown Prosecutor and asked that the victim be advised of this information.

Investigate the Breach

- [22] On Friday September 1, 2017, the Lawyer listened to the DVD victim's statement on a work issued laptop while driving to Wynyard. The Lawyer arrived at the Wynyard Courthouse before 10:00 a.m. and left the laptop in the vehicle while in court. He then returned to the vehicle at noon and drove to get lunch and parked the vehicle in downtown Wynyard. Then drove back to the court house and parked the vehicle there. At approximately 5:30 p.m., before leaving Wynyard, the Lawyer bought gas at the local Esso and picked up supper at the Subway. On his drive back to Regina, he stopped briefly at the Dafoe rest stop. When he arrived in Regina, he parked the car in his locked garage for the weekend.
- [23] Upon arrival at SLAC on Monday September 4th, he discovered the laptop was missing from his vehicle. As the car does not appear to show any evidence that it was broken

into, the Lawyer believes he accidentally left the car unlocked at some point during the day on Friday September 1, 2017 while in Wynyard.

[24] SLAC advised that the laptops are used for clients and Lawyers to review disclosure and do not contain any SLAC information or have access to the SLAC server. The laptop was password protected, but the DVD inside the laptop that contains the personal information/personal health information of the victim was not encrypted and/or password protected.

[25] In the draft report, my office recommended that SLAC explore options to encrypt and password protect storage devices (including USB keys, CD, DVD, etc.) to ensure sensitive information is appropriately safeguarded.

[26] SLAC responded indicating their USBs are encrypted, however the DVD at issue in this matter was received from the Provincial Crown Prosecutor through disclosure. Disclosure if provided from that office in a number of different mediums including DVD, USB and paper. SLAC advised it would undertake discussions with the Provincial Prosecutor's office to increase the security of the information provided.

[27] While I encourage SLAC to have these discussions with the Provincial Crown Prosecutors office, SLAC also has responsibility to ensure proper safeguarding of the information in its possession. It is recommend that SLAC ensure storage devices received that contain personal information and/or personal health information are properly encrypted and/or password protected, especially when transporting these devices outside of the office.

[28] Appendix A of SLAC's Client Information Management Policy provides the following regarding safeguarding of personal information when outside of the office:

When transporting files, diaries, computers or cell phones between one's home, office and courts,

- i. Files, diaries and computers must be transported in a locked briefcase. Legal Aid Saskatchewan will supply Lawyers and legal assistants with appropriate briefcases, as needed.
- ii. The briefcase must not be left in an unlocked vehicle.
- iii. The briefcase must not be left in a vehicle overnight.
- iv. When left in a locked vehicle during the day, the briefcase must be placed in the trunk or backseat footwell or other less visible position. The vehicle should be parked in a secure location. This arrangement should only be in place for brief periods.

[29] When my office followed up with SLAC, it advised the laptop was left on the front seat of the vehicle and was not in a locked briefcase. SLAC also indicated in its report that the Lawyer believes he had mistakenly left the car unlocked. Further, the Lawyer would have left the laptop in the vehicle all weekend.

[30] None of the safeguards provided in this policy were followed by the Lawyer.

[31] In my office's Investigation Report 103-2017, my office indicated that unless there are no other alternatives, records should never be left unattended in a vehicle while the employee is elsewhere. In my office's draft report, it was recommended that SLAC revise its policy to provide that records be kept under the constant control of the employee including meals and other breaks. If this is not possible, the records should be temporarily stored in a secure location such as a locked room or desk drawer.

[32] SLAC responded indicating lawyers are sent to court with multiple briefcases of paper files and in many remote locations court is held in a public location (such as a curling rink, band hall, etc.) and do not have access to a secure location to store the information.

[33] SLAC indicated it was not reasonable for a lawyer to carry multiple briefcases with them into a restaurant but do ask that they do their best to park in a location visible from the restaurant.

[34] When I recognize the obstacles faced by SLAC when transporting large amounts of paper, the personal information/personal health information in this case was stored on a DVD. A DVD is not a large item. The Lawyer should have, and easily could have,

carried the DVD with him at all times to ensure it was secure. SLAC Lawyers should be well aware, not only of their obligations under FOIP and HIPA, but based on their professional responsibilities be aware of the importance of maintaining confidentiality. Leaving the DVD with the personal information/personal health information of the affected individual in the unlocked vehicle was a sloppy practice.

[35] In the resource *Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office* from the Information and Privacy Commissioner of Ontario, it provides that “to prevent loss or theft, a disk or CD should be carried in a locked briefcase and kept under constant control of the employee while in transit.” In The Canadian Bar Association resource *Legal Ethics in a Digital World: CBA Ethics and Professional Responsibility Committee* it provides:

...if confidential data is carried out of the office, encryption mechanisms should be adopted to secure it during transport. In fact, when possible, it is safer to access information through a secure VPN connection than to carry files on a laptop hard drive or USB key.

[36] In my draft report, I recommended that SLAC explore the possibility of Lawyers using a secure VPN connection to access records that contain personal information/personal health information, rather than transporting paper or storage devices that contain this information. Alternatively, it was recommended that any records transported outside of the SLAC office be stored on an encrypted and password protected storage device that is kept with them at all times in a locked briefcase.

[37] SLAC responded that lawyers currently have access to electronic files through a secure VPN connection. SLAC also indicated it was in the process of improving its IT infrastructure to allow for more comprehensive use of electronic files with the intent for lawyers to carry less paper material to court. Further, SLAC indicated it was revising its IT Security Policy to provide that laptops, tablets and phones must not be left in cars.

[38] I applaud SLAC for these changes and encourage them to continue to pursue IT options to reduce the amount of paper that lawyers need to transport outside of the office. As

well, I recommend that SLAC's revisions to its IT Security Policy provide that not only the mobile devices not be left in vehicles, but ensure those devices are kept with the employee at all times in a locked briefcase. SLAC should also ensure that the policy provides the same protection for any storage devices, such as a DVD or USB.

Prevent future breaches

[39] SLAC indicated a written reprimand was recommended for the Lawyer involved. As well, all staff Lawyers would receive a reminder to secure phones, diaries, laptops and client files appropriately when outside of the office.

[40] My office asked SLAC how often employees receive privacy training. SLAC advised all employees received in-person privacy training in 2015 at the annual staff conference/professional development day. SLAC were planning to provide privacy training to employees at this conference every three years. New employees also complete the Access and Privacy Course for Saskatchewan Government Employees.

[41] My office, in many other reports, recommended that public bodies implement a program of mandatory annual training for all employees. In my draft report, it was recommended that SLAC also adopt this recommendation.

[42] SLAC responded indicating it would be developing an online training module for all employees to complete annually. It would also keep a record to ensure all employees successfully complete the module.

Privacy Breach Report

[43] This final step is ensuring all information collected is included in an internal privacy breach report. SLAC provided my office with its internal investigation report on September 25, 2017 detailing steps taken to respond to this breach.

III FINDING

[44] I find SLAC responded appropriately to the privacy breach.

IV RECOMMENDATIONS

[45] I recommend SLAC ensure all mobile devices and storage devices that are transported outside of the office are properly encrypted and password protected and kept with the employee at all times in a locked briefcase.

[46] I recommend SLAC continue to pursue IT options, including improvements to its current secure VPN connection, to reduce the amount of paper records lawyers need to transport outside of the office.

Dated at Regina, in the Province of Saskatchewan, this 23rd day of October, 2017.

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