Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 243-2017

Public Service Commission

May 18, 2018

Summary: On June 23, 2017, the Complainant submitted a privacy breach complaint to the Public Service Commission (PSC). The Complainant alleged that PSC had inappropriately shared their personal health information. PSC responded to the Complainant indicating that no breach of privacy had occurred. On September 29, 2017, the Complainant submitted a request for investigation to my office. The Information and Privacy Commissioner (IPC) found that PSC had not appropriately applied the data-minimization principle when disclosing the Complainant's personal information. The Commissioner recommended PSC ensure its policies or procedures for using and disclosing personal information and/or personal health information, when managing employee absences, consider the need-to-know and data minimization principles.

I BACKGROUND

[1] On June 23, 2017, the Complainant submitted a privacy breach complaint to the Public Service Commission (PSC). The Complainant alleged that PSC had inappropriately shared their personal health information.

[2] On September 22, 2017, PSC responded to the Applicant's alleged breach of privacy complaint indicating that no privacy breach had occurred.

[3] On September 29, 2017, my office received a request from the Complainant to investigate this alleged breach of privacy incident.

[4] On October 10, 2017, my office notified the Complainant and PSC of my office's intention to undertake an investigation into the alleged breach of privacy. My office requested a copy of PSC's internal investigation report, details of PSC's consideration of the need-to-know and data minimization principles and copies of any relevant policies or procedures.

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?

[5] The alleged breach of privacy complaint is regarding use and/or disclosure of the Complainant's information when managing the Complainant's absence from work. While PSC had been requesting medical information from the Complainant's doctor regarding the absence, there was also information regarding the Complainant's employment with PSC.

[6] A government institution is defined at subsection 2(1)(d) of FOIP. Subsection 2(1)(d)(ii) of FOIP provides:

> **2**(1) In this Act:
> …
> (d) **"government institution"** means, subject to subsection (2):
> …
> (ii) any prescribed board, commission, Crown corporation or other body…

[7] PSC is prescribed as a government institution in Schedule 1 of *The Freedom of Information and Protection of Privacy Regulations* (FOIP Regulations).

[8] PSC is also considered a trustee pursuant to 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 type of information PSC was considering when managing the Complainant's absence, it appears both personal information and personal health information were involved.

[11] As such, I find that both FOIP and HIPA apply.

2. Did PSC appropriately apply the need-to-know and data-minimization principles when using and disclosing the Complainant's personal information and/or personal health information?

[12] In the request for investigation submitted to my office, the Complainant indicated that the alleged breach of privacy involved at least two employees in PSC's Employee Service Center (ESC). The Complainant also provided my office with a number of copies of correspondence showing the different parties involved in the management of their absence.

[13] In the complaint to both PSC and my office, the Complainant was particularly concerned with a February 16, 2017 letter received from the Manager, Business Management and Planning as the Complainant did not believe the Manager had a need to know this information. Upon reviewing the copies of correspondence the Complainant had provided to my office, my office also requested PSC address two other points. This involved PSC's consideration of the need-to-know and data minimization principles for information disclosed to the Complainant's doctor and the role that each PSC employee played in the management of the employee's absence from work.

[14] The *IPC Guide to HIPA* provides the following definitions for the need-to-know and data minimization principles:

> **Need-to-know principle**
>
> The need-to-know principle is self-explanatory. Trustees and their staff should only collect, use or disclose personal health information needed for the diagnosis, treatment or care of an individual. Personal health information should only be available to those employees in an organization that have a legitimate need-to-know that information for delivering their mandated services. A trustee should limit collection and use of

> personal health information to what he/she needs-to-know to do his/her job, not collect or use information that is 'nice to know.'
>
> **Data minimization principle**
>
> The data minimization principle means that a trustee should collect, use or disclose the least amount of identifying information necessary for the purpose.

[15] Public bodies should ensure they are considering both the need-to-know and data minimization principles when using and disclosing personal information/personal health information. Use and disclosure are terms that are defined in my office's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities*:

> **Disclosure**: A privacy breach could occur when an unauthorized disclosure of personal information transpires (e.g. when personal information is missing, when an employee accesses personal information without a need-to-know, when a public body shares personal information with another organization, etc.). Note: if personal information in the possession or control of a public body is missing, even if there is no evidence that someone has viewed the personal information, it qualifies as a disclosure. The rules for disclosure are found in section 29 of FOIP...
>
> **Use**: A privacy breach could occur when personal information already in the possession or control of the public body is used for reasons that are not consistent with the purpose for which they were collected (e.g. personal information is collected to provide one service and then used to promote a different service). The rules for use are found in section 28 of FOIP...

[16] I will first consider the use of the Complainant's personal information/personal health information, and then address the disclosure.

Use

[17] While managing the Complainant's absence from work, seven PSC employees were included in the correspondence at different points of the Complainant's absence. This included the Complainant's two Managers, two Human Resource Consultants, a Senior Labour Relations Consultant, the Executive Director of ESC and the Manager, Business Management and Planning acting on behalf of the Executive Director for a period of time.

[18] My office asked PSC to explain the role each individual had in the management of the Complainant's absence from work, what information each individual had access to, and whether or not the need-to-know and data minimization principles were considered.

[19] PSC advised that the two Human Resource Consultants were the direct contact with the doctor and would have been the only PSC employees to receive the Complainant's personal health information. My office was advised that the only employee the Human Resource Consultant shared any of the Complainant's personal health information with was the Labour Relations Consultant. PSC explained certain pieces of the Complainant's personal health information were shared with the Labour Relations Consultant to provide the Human Resource Consultants assistance on workplace accommodation requirements and contractual guidance.

[20] As noted earlier in this report, the Complainant was particularly concerned with the February 16, 2017 letter signed by the Manager, Business Management and Planning. PSC advised that the Manager was acting on behalf of the Executive Director whom was away from the office. PSC was awaiting additional medical information from the Complainant in order to determine the status of the Complainant's absence. Prior to the Executive Director's absence from the office, the Manager was provided a verbal update on the Complainant. This included the name of the Complainant, status of their employment, accommodation request and duty of the employer to determine appropriate outcomes.

[21] The Manager was also advised that the Complainant's status could change if sufficient medical information was provided. The Manager was advised that if the Human Resources consultant did not receive sufficient medical information, a letter would need to be sent advising the Complainant that they would be placed on leave without pay. If sufficient medical information was provided, then the Manager would be responsible to ensure appropriate accommodations were in place for the employee's return to work.

[22] Both the Executive Director and the Manager indicated they were not provided with any of the Complainant's personal health information. The Complainant's two Managers also indicated they were never provided any of the Complainant's personal health information.

[23] Based on the information provided by PSC, it does not appear PSC inappropriately used the Complainant's personal health information in the management of the Complainant's absence.

Disclosure

[24] In correspondence dated January 10, 2017, February 1, 2017 and March 9, 2017 addressed to the Complainant's doctor, PSC including information surrounding the employee's work performance and that the employee had been placed on a performance improvement plan.

[25] My office asked that PSC explain how the need-to-know and data minimization principles were applied when determining what information was required to disclose for the management of the employee's absence in these cases.

[26] PSC responded indicating that PSC had disclosed this information to the Complainant's doctor for consideration when responding to the request for medical information. Based on information from PSC, it appears PSC learned of the Complainant's concerns about their work environment in February 2017. This information was provided through a meeting with the Complainant and medical information provided to PSC by the Complainant's doctor. PSC indicated that additional detail about the Complainant's work environment was provided to the Complainant's doctor in the March 9, 2017 letter in order to determine an appropriate course of treatment and try to accommodate a return to work for the Complainant.

[27] From the information provided to my office, it does not appear PSC was initially aware that the Complainant's absence was related to the work environment. While it may have been necessary for PSC to disclose information to the doctor regarding the Complainant's work environment and performance at work in the subsequent requests for information, it is not clear why PSC would have needed to disclose this type of information in the initial request for medical information from the doctor.

[28] In response to the draft report, PSC responded stating that often when employees are on performance improvement plans and are requesting medical leave, additional information from the employee's doctor is required. In an effort to reduce the frequency that PSC has to contact the doctor, information regarding the workplace will be provided at the onset. PSC also noted that employees are provided the request for medical information which they are responsible for providing to the physician to allow PSC to obtain sufficient medical information for their absence. PSC took the position that because the employee never raised an objection to the information in the correspondence, this was considered implied consent.

[29] The *IPC Dictionary* provides the following definitions of consent and implied consent:

> **Consent** – informed, voluntary agreement with what is being done or proposed with respect to the collection, use or disclosure of personal information.
>
> **Implied consent** must first meet a number of conditions. The consent to the collection, use or disclosure of personal health information by a trustee may only be implied if:
>
> - In all circumstances, the purpose of the collection, use or disclosure is or will become reasonably obvious to the individual.
> - It is reasonable to expect that the individual would consent to the collection, use or disclosure.
> - The trustee is not aware that the individual withdrew consent.
> - The trustee uses or discloses the information for no other purpose other than the purpose for which it was collected.
> - The individual has the right to "opt out".

[30] The personal information that was disclosed to the employee's doctor was related to the employee's work performance. It is not clear how PSC reached the conclusion that it would be reasonably obvious to the employee that this information could be disclosed for the purposes of gaining sufficient medical information related to their absence.

[31] Additionally, based on copies of correspondence provided by the Complainant, the emails forwarding the medical information request for the doctor, does not provide the employee with any indication that they are able to contact PSC if they are concerned with the information being disclosed. PSC has obligations under FOIP and HIPA for the collection,

use and disclosure of personal information/personal health information. Regardless if PSC has express or implied consent, or has authority under FOIP/HIPA for the collection, use or disclosure of an individual's personal information/personal health information, PSC has an obligation to consider the need-to-know and data minimization principles.

[32] I find that PSC did not appropriately apply the data minimization principle when disclosing personal information to the Complainant's doctor.

[33] I recommend PSC ensure its policies or procedures for using and disclosing personal information and/or personal health information, when managing employee absences, consider the need-to-know and data minimization principles.

III FINDINGS

[34] I find that FOIP and HIPA apply.

[35] I find that PSC did not appropriately apply the data minimization principle when disclosing the Complainant's personal information to the Complainant's doctor.

IV RECOMMENDATION

[36] I recommend PSC ensure its policies or procedures for using and disclosing personal information and/or personal health information, when managing employee absences, consider the need-to-know and data minimization principles.

Dated at Regina, in the Province of Saskatchewan, this 18th day of May, 2018.

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