Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 224-2016

Ministry of Highways and Infrastructure

April 20, 2017

Summary: The Ministry of Highways and Infrastructure (Ministry) reported to my office that a box of records containing 19 inactive employee records was missing from its Kindersley District Office. Through the course of its investigation, the Ministry learned that the missing records may have been accidentally shredded. However, without an inventory of records or other evidence that the employee records were destroyed, the Commissioner was unable to conclude that the records were shredded and not inappropriately taken from the office. The Commissioner found a number of inadequacies in the Ministry's investigation of this breach of privacy and its records management practices. Further, the Commissioner found the Ministry did not meet its duty to protect under section 16 of *The Health Information Protection Act* (HIPA). The Commissioner recommended the Ministry provide written notification to the 19 affected individuals. The Commissioner also recommended the Ministry further investigate the possibility of the records being inappropriately taken from the Kindersley District Office. Finally, the Commissioner recommended the Ministry update his office as it completes each phase of its Records Management Project Charter towards compliance with *The Archives and Public Records Management Act*.

I BACKGROUND

[1] On September 6, 2016, the Ministry of Highways and Infrastructure's (Ministry) Kindersley District Office received a request for copies of time card records from the Provincial Auditor's Office. This prompted the District Office Coordinators (Coordinators) to search for the records. During the search, the Coordinators noticed that

a box of records containing inactive employee records was missing. A search of the office was conducted and the records were not found.

[2] On September 13, 2016, the Acting District Operations Manager from the Kindersley District Office contacted my office, as well as the Public Service Commission seeking advice. The Ministry's privacy office was notified of the potential breach.

[3] On September 14, 2016, the Ministry proactively reported the breach to my office and my office notified the Ministry that it would be monitoring the matter.

[4] On December 21, 2016, it was determined that my office would commence a formal investigation into the matter.

II DISCUSSION OF THE ISSUES

[5] The Ministry is a "government institution" as defined in subsection 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP) and a "trustee" of personal health information as defined in subsection 2(t)(i) of *The Health Information Protection Act* (HIPA).

1. Does the information qualify as personal information under FOIP and/or personal health information under HIPA?

[6] As noted above, the Coordinators noticed that a box of records containing 19 inactive employee records was missing. The Ministry advised my office that these employee records would contain information such as employee commencement forms, classification reviews, leave of absence information, long term disability claims, sick leave doctor notes, disciplinary documentation, etc.

[7] Subsection 24(1) of FOIP defines "personal information" and provides:

> **24**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form….

[8] Subsections 24(1)(a) through (k) provides examples of types of personal information. However it is a non-exhaustive list.

[9] In order to qualify as personal information, the information needs two elements present – it must be about an identifiable individual and it must be personal in nature:

1. *Identifiable individual* means that it must be reasonable to expect that an individual may be identified if the information were disclosed. The information must reasonably be capable of identifying particular individuals because it either directly identifies a person or enables an accurate inference to be made as to their identity when combined with other available sources of information (data linking) or due to the context of the information in the record.

2. *Personal in nature* means that the information reveals something personal about the individual. Information that relates to an individual in a professional, official or business capacity could only qualify if the information revealed something personal about the individual (such as employment history).

[10] Based upon the description of the records at issue, some of the information contained within these records would meet the two elements outlined above. This would include information found in employee commencement forms, leave of absence information, and disciplinary documentation. Therefore, I find that this would qualify as personal information under FOIP.

[11] HIPA is engaged when three elements are present: 1) a trustee, 2) personal health information, and 3) the trustee must have custody or control over the personal health information.

[12] First, the Ministry qualifies as a trustee as provided under subsection 2(t)(i) of HIPA. Second, based on the description of the employee records given by the Ministry, the files that are missing may have contained personal health information as defined by subsection 2(m) of HIPA. This would include the type of information you would find in employee disability claims and sick leave notes from a physician. Third, as the personal health information is contained within Ministry employee records, the Ministry has custody of the records. Therefore, I find that HIPA is also engaged.

2. Did the Ministry follow best practices in its response to the alleged breach of privacy?

[13] When a privacy breach has occurred, my office's resources *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Trustees* each recommend five best practice steps to be taken by public bodies when responding to privacy breaches. These are:

1. Contain the breach,
2. Notify affected individuals and/or appropriate organizations,
3. Investigate the breach,
4. Prevent future breaches, and
5. Prepare a privacy breach report.

Contain the breach

[14] Upon learning that a privacy breach has occurred, public bodies should immediately take steps to 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 or electronic security.

[15] As noted above, the Ministry contacted my office on September 13, 2016. The Kindersley District Office believed that the office was accessed after hours, therefore on September 14, 2016 its locks were changed at the front and rear office entry doors and a new locking file cabinet was ordered.

[16] In its submission, the Ministry advised that a course of action had been agreed upon, which included contacting the 19 inactive employees whose personal and personal health information was missing. The Ministry also planned to hire a private investigator to look into this issue, as there were internal issues between staff at the time and it was felt that an outside perspective was needed.

[17] The Ministry's Privacy Officer and the Acting District Operations Manager began to interview administrative staff at the Kindersley District Office about the missing employee records.

[18] During the same time the Ministry was conducting the interviews, it was suggested that the missing employee records could have been inadvertently shredded. The Ministry advised my office that the Coordinators were engaged in a records clean-up that began in November 2015. Through the records clean up, approximately 100 boxes were identified for shredding. An index of records was not prepared for the 100 boxes.

[19] At first, the records were being shredded onsite by staff of the Kindersley District Office. However as the onsite shredding was proceeding at a slow pace, the decision was made to hire a shredding company to shred the remaining records onsite. The Ministry provided my office with a copy of a June 17, 2016 invoice from a private shredding company detailing that 49 bankers/archive boxes were shredded on site on that date.

[20] Because of this new development, the Ministry did not proceed with investigating or hiring a professional investigator. In addition, the 19 employees whose employee records were missing were not notified.

[21] I recognize that the 49 boxes being shredded would have increased the probability that the employee records were inadvertently shredded. However, the Ministry cannot conclusively determine if the 19 employee records had actually been destroyed during the shred because there was not an inventory of records prepared or tracking of what records were destroyed and no employee could attest to the fact that those records were included. I will be discussing the Ministry's records management practices later in this report.

[22] Lacking an inventory of records or other evidence that the employee records were destroyed, I cannot conclude that the Ministry has properly contained the breach of privacy.

Notify affected individuals and/or appropriate organizations

[23] Notifying an individual that their personal information or personal health information has been inappropriately accessed 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 access. Unless there is a compelling reason not to, public bodies should always notify affected individuals.

[24] In addition to notifying individuals, public bodies may want to notify other organizations, for example, my office, law enforcement or other regulatory bodies that oversee particular professions.

[25] My office was notified about this potential breach of privacy on September 13, 2016. However, the Ministry has not notified the 19 employees whose employee records are missing. As the possibility exists that the employee records were removed from the Kindersley District Office without authorization, the Ministry should notify the affected individuals about what occurred. This will allow those 19 employees to take appropriate steps to protect themselves from possible identity theft, humiliation, and damage to reputation.

Investigate the breach

[26] The next step in responding to an alleged privacy breach is to investigate. Upon learning of the missing employee records, office staff was interviewed by the Ministry's Privacy Officer and the Acting District Operations Manager.

[27] The Ministry informed my office that around the time the interviews were being conducted, one of the District Office Co-ordinators advised senior officials in the Ministry that the employee records may have accidentally been shredded. The Ministry did not continue its investigation once it was discovered that the employee records may have been shredded.

[28] I am concerned that the Ministry immediately accepted that the employee records were shredded, rather than continuing to investigate the inappropriate removal of the records from the Kindersley District Office. Lacking further evidence – such as an index of records outlining what was in fact was destroyed – it would be impossible for the Ministry to come to this conclusion with certainty.

[29] Nevertheless, this is the approach the Ministry took. However it should reconsider the possibility that the employee records were taken and not destroyed and investigate this incident further.

[30] Once learning of the possible destruction of the employee records, the focus was shifted to that of inappropriately disposing of the files. This included the request of records retention schedules, file keys, destruction authorization and the Certificate of Destruction. Staff was only able to provide the Certificate of Destruction, which showed that 49 boxes were shredded on June 17, 2016.

[31] I recognize the probability of destruction increased once learning that the office disposed of 49 boxes. However, as the Ministry did not have an inventory of records I am not satisfied that they provided sufficient evidence that the employee records were in fact destroyed.

[32] Through this investigation, my office has learned that the Ministry did not have appropriate records management policies and procedures in place. The Ministry advised that the 19 employees whose files were missing were no longer employed by the Ministry. Their employment end dates ranged from May 2010 to November 2015.

[33] According to the *Administrative Records Management System* (ARMS) 2014, which all provincial Ministries are bound by, employee records are classified under 1415 – Employee Record. Section 1415 of ARMS describes the type of information found in an employee record:

> Records documenting employee work history such as personal data, resumes, oaths, work plans and appraisals of job performance, work histories, skills, training and education, commendations and discipline.
>
> Includes: Employee File (by employee), Pay Records, Hours of Work (by employee), Seniority Calculations, Long-term disability, Designated Paid Holidays, Special and Other Types of Leave, etc.

[34] It appears from the description of the employee records at paragraph [6], that at least some of the employee records would qualify under section 1415 of ARMS. Section 1415 of ARMS also sets the retention period for an employee record:

> Age 75 of employee or 5 years after death (whichever is earlier) provided 5 years have elapsed since the last administrative action on the file.

[35] As the employee end dates ranged from May 2010 to November 2015, it is highly unlikely that any of the employee records were eligible for disposal when the onsite shredding took place (June 2016). Even if the records were eligible for disposal, my office was advised by the Provincial Archives that the Ministry was not granted permission to dispose of any records during the time the possible shred took place, nor had they received a request for destruction from the Kindersley District Office.

[36] *The Archives and Public Records Management Act* (APRMA) outlines that the Provincial Archivist of Saskatchewan must grant permission for public records to be disposed of. Subsection 18(2)(j) of APRMA provides:

> **18**(2) Without limiting the generality of subsection (1), the Provincial Archivist may do all or any of the following:
>
> …
>
> (j) subject to any term or condition pursuant to which a record has been acquired or obtained, direct that the record be destroyed or otherwise disposed of if the Provincial Archivist has determined that the record no longer has archival value.

[37] The failure to undertake an inventory of the employee information and seek permission from the Provincial Archivist to destroy the records (if they were in fact destroyed) meant a failure to safeguard and properly dispose of the employee records. This action is a contravention of section 22 of APRMA which provides:

> **22**(1) Subject to subsection (2), no person shall, with an intent to deprive the Government of Saskatchewan, a government institution or the Provincial Archives of Saskatchewan of the custody, control or use of, or access to, a public record:
>
> (a) destroy or damage the public record;
>
> (b) remove or conceal the public record from the Government of Saskatchewan, a government institution or the Provincial Archives of Saskatchewan; or
>
> (c) direct, counsel or cause any person in any manner to do anything mentioned in clause (a) or (b).

[38] If the employee records were destroyed, the Ministry was in contravention of its responsibilities under APRMA.

[39] In addition, based on the records description, the employee records contained personal health information, therefore the Ministry has custody of personal health information under HIPA. As such, the Ministry has a duty under HIPA to protect the personal health information pursuant to Parts III and IV of HIPA. In particular, section 16 of HIPA requires the Ministry to have administrative, technical and physical safeguards in place. These safeguards must protect against any reasonably anticipated threat or hazard to the security or integrity of the information; and the loss of, unauthorized access to, use or disclosure of the information. Section 16 of HIPA provides:

> **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.

[40] Furthermore, subsection 17(2) of HIPA requires a trustee to have a retention and destruction schedule in place for its personal health information, and provides:

> **17**(2) A trustee must ensure that:
>
> (a) personal health information stored in any format is retrievable, readable and useable for the purpose for which it was collected for the full retention period of the information established in the policy mentioned in subsection (1); and
>
> (b) personal health information is destroyed in a manner that protects the privacy of the subject individual.

[41] As it relates to the personal health information contained within these records, if the employee records were inappropriately removed from the Kindersley District Office, the Ministry is in violation of section 16 of HIPA. Further, if in fact the records were inappropriately destroyed, the Ministry is in violation of sections 16 and 17 of HIPA.

[42] I would like to emphasize that the requirement for government institutions to have proper records retention and disposition practices in place is not a new responsibility. In 1993, the Saskatchewan Archives Board developed the Saskatchewan Administrative Records System which was a records classification and records retention system to be adopted by all government institutions. This has evolved into what is now the Administrative Records Management System, 2014, and I encourage all government institutions to adopt this system to ensure compliance with APRMA.

[43] The Ministry advised that on September 29, 2016, a Records Management Unit was created within the Ministry to meet the records management obligations under APRMA. The Ministry also adopted a Records Management Project Charter (Charter) in September of 2015, where the target is to achieve full compliance with APRMA by January 2020. Since the adoption of the Charter, the Ministry advises they have been working with the Saskatchewan Archives Board in regards to its records management obligations.

[44] I am encouraged that the Ministry is working towards compliance under APRMA by the establishment of the Records Management Unit and that it has adopted the Records Management Project Charter. I trust this will help to mitigate the risk of incidents such as this happening in the future.

[45] I find that the Ministry did not conduct an adequate investigation.

Prevent Future Breaches

[46] Once a privacy breach has occurred, a very important step is to implement measures to prevent future breaches from occurring. Part of this process is to determine the steps that can be taken to prevent a similar privacy breach:

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

[47] Upon learning of this potential breach, the Ministry changed the locks at the Kindersley District Office. The Ministry reminded Kindersley District Office staff and all administrative staff across the Ministry of the importance of keeping sensitive records locked at all times. The Ministry should go a step further and remind all staff of the Ministry about the expectation of handling sensitive records.

[48] The Ministry has provided my office with a copy of the above referenced *Records Management – Compliance with The Archives and Public Records Management Act, 2015 - Project Charter* (Project Charter) dated September 2015. The Project Charter sets eight phases for this project with a projected completion of 2020.

[49] Phase 5 outlines a staff training component. The Ministry should ensure that all staff is provided training and awareness surrounding their records management obligations.

Prepare a privacy breach report

[50] The final step in responding to an alleged privacy breach is to formalize what was discovered through the previous four steps by preparing a privacy breach report.

[51] The Ministry provided my office with a summary report of its investigation. However, I found inadequacies in the Ministry's investigation and response to the alleged privacy breach. Going forward, I would suggest the Ministry utilize my office's resources *Privacy Breach Guidelines for Government Institutions and Local Authorities* and *Privacy Breach Guidelines for Trustees* when conducting an investigation and preparing a breach of privacy report.

[52] I find the privacy breach report to be inadequate.

[53] Upon reviewing my office's draft Investigation Report, the Ministry advised it intends to comply with the Recommendations at paragraphs [61] and [63]. Further, it advised my office that it will explore the appropriate next steps concerning my Recommendation at paragraph [62].

III FINDINGS

[54] I find the Ministry did not meet its duty to protect under section 16 of HIPA.

[55] I find the Ministry did not meet its duty to have retention and destruction schedules under section 17 of HIPA.

[56] I find the Ministry did not properly contain the breach of privacy.

[57] I find the Ministry did not provide notification to the affected individuals.

[58] I find the Ministry's investigation of this breach of privacy to be inadequate.

[59] I find the Ministry's privacy breach investigation report to be inadequate.

[60] I find the Ministry's records management practices regarding the retention and destruction of records to be inadequate.

IV RECOMMENDATIONS

[61] I recommend the Ministry provide written notification to the 19 affected individuals of the privacy breach so they are aware of this incident.

[62] I recommend the Ministry further investigate the possibility of the records being inappropriately taken from the Kindersley District Office.

[63] I recommend that the Ministry update my office when it completes each of the eight phases of the Project Charter towards compliance with APRMA and meet its project completion target of January 1, 2020.

Dated at Regina, in the Province of Saskatchewan, this 20th day of April, 2017.

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