Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 271-2017

Ministry of Corrections and Policing

May 7, 2020

Summary: The Ministry of Justice proactively reported a breach of privacy to the Commissioner. During the course of the investigation correctional centres in the province moved from the Ministry of Justice to the Ministry of Corrections and Policing (Ministry). A Corrections Officer (CO) with the Saskatoon Correctional Centre (SCC) left an inmate file on a unit's food cart and as a result, inmates were able to view the file and remove portions of the contents of the inmate's file. Due to the CO's negligence, after viewing the file contents, two inmates assaulted the inmate and the inmate died as a result of the injuries. The Commissioner had a number of findings, which included the Ministry did not contain the breach and the notification efforts were insufficient; however, the Ministry conducted an adequate privacy investigation and took steps to prevent the risk of this type of breach happening in the future. The Commissioner made a number of recommendations to the Ministry, including that the Ministry consider implementing incident response steps and a notification process when a breach of privacy involves an inmate. The Commissioner recommended that the Ministry implement a policy change that the transportation of inmate files be a stand alone practice. The Commissioner recommended amendments to the *Ministry of Corrections and Policing Code of Professional Conduct* and the *Oath or Declaration of Office* and recommended that each be signed by employees annually. Further the Commissioner recommended correctional centre staff complete mandatory annual refresher privacy training and track its completion for each staff member. Finally, the Commissioner recommended that the Ministry provide a copy of this Investigation Report to the deceased individual's next of kin.

I BACKGROUND

[1] At the time this breach of privacy was reported to my office, the Ministry of Justice was a single ministry. However, on February 2, 2018, the Ministry of Justice was split into two ministries: the Ministry of Justice and the Ministry of Corrections and Policing. This matter now falls under the Ministry of Corrections and Policing. Therefore, this Report will refer to the Ministry of Corrections and Policing (Ministry).

[2] On October 30, 2017, the Ministry contacted my office to proactively report an alleged breach of privacy. The Ministry advised that some inmates at the Saskatoon Correctional Centre (SCC) were able to access another inmate's file, and something in the file caused them to assault that inmate.

[3] On November 3, 2017, my office notified the Ministry that we would be conducting an investigation on this matter. Due to the criminal investigation that was also underway, we advised the Ministry that it could provide us with updates on the status of the investigation every three months.

[4] Further, as the alleged breach of privacy was now an active criminal investigation, my office determined that it would not issue a report on this matter until the criminal matters were concluded, as to not impede the Court process.

II DISCUSSION OF THE ISSUES

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

[5] The Ministry is a "government institution" pursuant to subsection 2(1)(d)(i) of FOIP. Further, the Ministry is a "trustee" pursuant to subsection 2(t)(i) of HIPA.

[6] This incident occurred because a Corrections Officer (CO) left an inmate's file on a food cart that inmates had access to. The Ministry advised my office that upon the file being

viewed by inmates, two pages of the criminal record of an inmate (Deceased Individual) went missing from their file.

[7] In order for FOIP to be engaged, there must be personal information as provided for in subsection 24(1) of FOIP. To qualify as personal information, the information must relate to an identifiable individual and the information must be personal in nature. In order for HIPA to be engaged, there must be personal health information of an identifiable individual pursuant to subsection 2(m) of HIPA.

[8] The Ministry advised my office that the breach of privacy involved the Deceased Individual's inmate program file. The following are the types of information found in an inmate's file:

- criminal record;
- warrant reports of current charges;
- current and historical case management information including offender information reports, inmate risk assessments, and inmate case plans;
- orientation to unit forms; and
- suicide screening documentation.

[9] The inmate file is that of a particular identifiable individual. Subsection 24(1) of FOIP provides examples of types of information that could be considered personal information. Specifically, subsection 24(1)(b) of FOIP provides:

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

[10] A criminal record of an identifiable individual, including the information that would be included in an individual's inmate program file qualifies as personal information under FOIP.

[11] The Ministry provided my office with a copy of the *Suicide Prevention Screening Guidelines* that is to be completed for each inmate upon admission to the SCC. This form asks several questions to assess if an inmate is a suicide risk and includes questions about the inmate's psychiatric history, drug or alcohol abuse and if the inmate has previously attempted suicide. This type of information would qualify as personal health information under subsection 2(m) of HIPA, which provides:

> **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;

[12] Therefore, both FOIP and HIPA are engaged and I have the authority to investigate this matter.

2. Did the Ministry respond appropriately to the privacy breach?

[13] I would first like to sadly point out that because of this breach of privacy, a death occurred. Therefore, before I determine if the Ministry appropriately responded to the privacy breach, it is first important to outline what occurred. Through the Ministry's investigation report and the Court transcripts from the sentencing hearings, the following took place on October 23, 2017:

- At approximately 6:40a.m., a CO with the SCC picked up the Deceased Individual's program file from the administration area.

- Once the CO retrieved the program file, they proceeded to the kitchen to pick up the breakfast food cart for the unit at approximately 6:42a.m. and placed the inmate file in the food cart. At approximately 6:50a.m., the food cart was brought to the unit's secure sally port for pick up by Domestic 1 (an inmate assigned to the kitchen work placement for the unit). The food cart was then taken to the unit kitchen where Domestic 2 was waiting for the food cart. Video surveillance confirms that Domestic 2 removed the Deceased Individual's program file from the cart and viewed its contents while in the kitchen.

- At approximately 7:23a.m., Domestic 1 went to the staff desk to return the Deceased Individual's file to the CO. The CO placed the file in the file cabinet. After the fact when questioned, the CO stated they did not look in the file to confirm what was in the file, if anything was missing or confirm whose file it was. It was later determined that the first two pages of the criminal record of the Deceased Individual were missing and those pages were never recovered.

- Breakfast was served by the Domestics from 7:24a.m. to 8:18a.m. The Domestics made extended stops at three inmate cells.

- After breakfast, some of the inmates on the unit were let out of their cells. The Deceased Individual, and two inmates (Inmate 1 and Inmate 2) were part of the group of inmates let out of cells at that time. The Deceased Individual made a phone call, and returned to their cell.

- At approximately 8:55a.m., Inmate 1 and 2 followed the Deceased Individual into their cell and video surveillance reviewed after the incident occurred showed Inmate 1 pull back their arm in a punching motion, and then there was a disturbance in the cell. Inmate 1 and 2 were in the cell for approximately 45 seconds and were both seen leaving the cell.

- The Ministry confirmed that Inmate 1 and 2 were in the cells that Domestic 1 and 2 made extended stops at during breakfast service.

- At approximately 11:00a.m., the Deceased Individual was called in order to take their medication. The Deceased Individual did not respond to the call, and when they were checked on by CO's, they were discovered under their covers, with their head covered in blood.

- The Deceased Individual was taken by ambulance to the hospital with an extensive brain injury. The Deceased Individual was put into a medically induced coma. Due to the extent of the brain injuries, they were taken off life support and died on November 2, 2017. The autopsy report revealed the cause of death was blunt force trauma to the head.

[14] Therefore, in this circumstance, the Deceased Individual's personal information and personal health information was disclosed because their program file was left in a place where it could be taken and viewed by other inmates without a legitimate need-to-know.

[15] Therefore, I find a privacy breach occurred.

[16] In circumstances where a government institution proactively reports a privacy breach, the focus for my office becomes one of determining whether the government institution appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that the Ministry took the privacy breach seriously and appropriately addressed it. My office recommends five best practice steps be taken when a government institution discovers a breach of privacy has occurred. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Prevent future breaches; and
5. Write an investigation report.

[17] I will now consider if the Ministry appropriately responded to this matter against these five best practice steps.

Step 1: Contain the Breach

[18] Upon learning that a privacy breach has occurred, a government institution 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 security.

[19] Effective and prompt containment reduces the magnitude of a breach and in some instances, the risks to an individual.

[20] The Ministry advised my office that Domestic 1 returned the file to the CO at approximately 7:23a.m. When interviewed, the CO indicated they "felt panicked" when the file was returned, however they thought the program file was only missing for a few seconds. The CO did not check the contents of the file to see if anything was missing. The CO indicated they forgot about the incident until approximately 2:30p.m. when they were engaged in a conversation with colleagues and the Assistant Deputy Director of Programs as to why the assault may have occurred.

[21] At that time it was confirmed that the program file was missing the first two pages of the criminal record of the Deceased Individual. The Ministry did not provide my office with the attempts made to search for and recover the two missing pages, therefore I am not able to comment on the search efforts, if any, to recover the pages. However, the two missing pages of the Deceased Individual's criminal record were never recovered.

[22] I am very troubled by the fact that a CO lost possession of an inmate's personal record containing extremely sensitive and personal information, was fully aware that the file was in the possession of another inmate for a period of time, and yet, did not open the file to see what was missing. This one step alone might have prevented their death.

[23] There was a 90 minute lapse from the time the file was returned to the CO to the time the assault took place. Had the CO reviewed the contents of the file and determined that the criminal record was missing, steps could have immediately been taken to protect the Deceased Individual. These steps could have included:

- conduct a risk assessment on the information that was viewed on the file to ascertain the necessary steps needed to protect the Deceased Individual;
- place the unit into an immediate lockdown;
- review the video surveillance tapes to track the actions of the inmates on the unit when the file was missing;
- interview inmates that may have been made aware of the contents of the criminal record based upon the video surveillance footage;

- search for the missing pages; and
- remove the Deceased Individual from the unit.

[24] Instead, it appears that the CO carried on with their work day for another seven hours until there were discussions as to what could have led to the assault.

[25] Due to passage of time and lack of immediate steps to contain the breach at the time it occurred, it appears that there are no further steps that the Ministry can take to contain this breach.

[26] Therefore, I find the Ministry did not contain this breach of privacy.

Step 2: Notify affected individuals and/or appropriate organizations

[27] Notifying an individual that their personal information and/or personal health information was 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, government institutions should always notify affected individuals. An effective notification normally should include:

- A description of what happened;
- A detailed description of the personal information that was involved;
- A description of possible types of harm that may come to them as a result of the privacy breach;
- Steps that the individuals can take to mitigate harm;
- Steps the organization is taking to prevent similar breaches in the future;
- The contact information of an individual within the organization who can answer questions and provide further information;
- A notice that the individuals have a right to complain to the Office of the Information and Privacy Commissioner; and
- Recognition of the impacts of the breach on affected individuals and an apology.

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

[29] The CO did not check the file when it was returned, report that the file was missing or make any attempt to contain the breach. As noted above, when the CO was later interviewed, they indicated that they thought the file was only missing for a few seconds. Whether or not the CO actually looked in the file to see that the pages were missing, the file was still in the possession of an inmate for a period of time. Therefore, as a result of this negligence, inmates were able to obtain information about the Deceased Individual that resulted in the inmate being assaulted. Should a breach of privacy such as this occur going forward in any of the province's correctional centres, the affected individual should immediately be notified.

[30] The Ministry proactively notified my office on October 30, 2017. However, as the assaults were criminal matters, I decided I would not issue a report on the matter until the Court proceedings concluded. Inmate 1 and 2 both pleaded guilty to the charges and the final sentencing hearing concluded in November 2019.

[31] As this was a criminal assault resulting in death, the Saskatoon Police Service was notified and investigated the matter.

[32] I find the Ministry's notification efforts to be insufficient as the Deceased Individual was not notified that the file was in the possession of another inmate for a period of time.

Step 3: Investigate the Breach

[33] Once the breach has been contained (or it is determined it cannot be contained) and appropriate notification has occurred, the government institution should conduct an internal investigation. The government institution's privacy officer generally conducts the investigation 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 systematic basis and should include a root cause analysis. 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.

[34] The Ministry provided its internal investigation report. Once the sentencing hearing of Inmate 1 and 2 concluded, my office sought additional details and clarification from the Ministry.

[35] As noted above, the breach of privacy was the result of a CO leaving the Deceased Individual's program file inside the inmate breakfast cart. Because of this, the two Domestics had access to the program file and were able share information about the criminal record with other inmates on the unit. Through interviews with the CO, the Ministry concluded that it believes this breach was unintentional, and that the program file was not intentionally left on the food cart.

[36] The Ministry advised my office that the CO acknowledged that they placed the Deceased Individual's program file in the food cart and then failed to search the cart once it arrived at the unit. Further, video footage confirmed that Domestic 2 had the file in their possession and can be seen going through the file.

[37] Upon review of the file approximately seven hours after the assault took place, staff were able to confirm that the first two pages of the criminal record check were missing and the pages were never recovered.

[38] The Ministry advised my office of the standard procedure when transporting files. Typically the files are safeguarded when in transit within the SCC and remain in the physical possession of a CO. It is the responsibility of the CO to ensure the inmate file is securely transported without incident from one area of the centre to another.

[39] The reason the CO provided for placing the program file in the food cart was that the unit is located on the SCC grounds and is separate from the main building (where the kitchen is). They had concerns that the wind could have blown the file off the cart.

[40] Further, CO's are expected to search all items entering the facility to avoid contraband entering the facility. The CO involved in the incident advised the Ministry that they were

unaware of a specific policy regarding search and transporting food carts, although they would generally search the food carts.

[41] My office asked the Ministry if a policy existed regarding the search of food carts at the time of the incident. The Ministry advised that there was not a policy specifically speaking to the searching of food carts. However, as a result of this incident it has changed the search plan and all staff have been informed about the requirement to search anything coming into the unit, including food carts.

[42] My office also inquired if it is the responsibility of the CO transporting the food cart to also search the food cart once it arrives to the unit. The Ministry responded that it is the responsibility of the staff on the unit who is accepting the cart, however, the CO transporting the cart could also be the same CO who is searching the cart.

[43] I do not believe this goes far enough. CO's should not be combining the duty of the transfer of inmate files to the particular unit with transferring of items that will be provided to inmates on the unit – including food carts. This practice – although saves time - heightens the risk of this type of breach happening again.

[44] The Ministry outlined the physical and administrative safeguards that were in place at the time the breach occurred. As this breach resulted from the disclosure of a paper file, technical safeguards are not engaged.

[45] The Ministry identified the physical safeguards being that inmate files are to be under the possession and control of staff at all times, including during transport. There are physical barriers in place including locked doors and cabinets to ensure that inmates do not have access to files on the unit. The file was not taken from the unit file room, therefore, I am satisfied that these physical safeguards are sufficient.

[46] The Ministry identified administrative safeguards it had in place for the CO. On November 2, 2009, the CO sign the *Oath or Declaration of Office* (Oath). In part, the Oath outlined that the CO would not "…use or disclose any matter or information that comes to my

knowledge by reason of my employment…." The CO did breach the Oath, even if unintentionally, by disclosing the information to the inmates.

[47] However, the Oath was signed by the employee eight years prior to the breach. In order for employees to be continually reminded about their access and privacy obligations, the Oath should be signed by employees on an annual basis.

[48] In addition, the Ministry shared paragraph 3 of the Oath with my office, which states:

> 3. That I will not use or disclose any matter or information that comes to my knowledge by reason of my employment, including personal information about any individual, unless:
>
> (a) that use or disclosure is permitted by *The Freedom of Information and Protection of Privacy Act*; and
>
> (b) I have authorization from my employer to make that disclosure.

[49] As outlined above, CO's, in addition to having access to personal information pursuant to FOIP, also have access to some personal health information pursuant to HIPA. Therefore, the Oath should be amended to include HIPA.

[50] I also note that on January 1, 2018, FOIP was amended. The amendments were passed after the breach of privacy occurred. Since the amendments, FOIP now includes an explicit duty to protect personal information. Section 24.1 of FOIP provides:

> **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.

[51] Section 16 of HIPA has a similar provision surrounding a trustee's duty to protect.

[52] The duty to protect personal information and personal health information in a correctional facility is something that staff should be reminded of on a regular basis. Therefore, the Ministry should amend the Oath to include employee's duty to protect obligations.

[53] The Ministry advised that correctional centre employees are required to review the *Ministry of Corrections and Policing Code of Professional Conduct* (Code) annually. The CO last signed the code on January 17, 2017, which was within the year of the breach occurring. The Ministry provided my office with a copy of the relevant sections of the Code:

> **Principles**
>
> - Respect and Integrity – Act at all times in a manner that will bear the closest public scrutiny
> - One Team – Conduct themselves in a professional manner that reflects positively on the Ministry of Justice, Corrections and Policing and the Saskatchewan Public Service generally.
>
> **Employee Expectations:**
>
> - Not using or disclosing any matter of information, according to the Oath and Declaration of Office, unless allowed by law and/or policy, that comes to their knowledge by reason of their employment.
> - Properly safeguarding and not removing any documents including but not limited to, log books, offender files, ledgers, reports, policies, manuals and any other written material published, distributed or circulated by the employer.
>
> …

[54] The portion of the Code that the Ministry provided to my office does not mention FOIP or HIPA. Although it outlines actions that align with the duty to protect, it does not specifically speak to employees' duty to protect obligations under FOIP and HIPA.

[55] So that employees are aware they have legal obligations under FOIP and HIPA, the Ministry should amend the Code to reflect those legal obligations.

[56] The Ministry provided me with the wording found on the Code signature page:

> By signing this document I am confirming that I have read and I recognize that it is my duty to follow this Commitment to Excellence & Code of Professional Conduct and I understand the consequences of not adhering to it. I understand that while I am not obligated to sign this document I am still obligated to comply with it.
>
> I will ensure that I fulfill my duties courteously and appropriately without malice or ill will, never employing unnecessary force or violence and never accepting improper gratuities.

[57] I am concerned that the signature page states, "*… I understand that while I am not obligated to sign this document I am still obligated to comply with it.*" If there are instances that CO's do not sign this form, how would supervisors have proof that the Code was in fact read by the CO each year? The Ministry should change this practice so that staff are required to not only review the Code, but also sign the Code on an annual basis.

[58] In regards to training that CO's receive, the Ministry advised my office that all SCC staff have access to the Saskatchewan Government's Access and Privacy self-directed learning module. As of 2014, all new staff attend in-person access and privacy training offered as part of the Induction Training Program (ITP) for Correctional Officers. The Ministry further advised that the CO completed ITP in 2009, but at that time the access and privacy training component was not included in the program.

[59] However, the Ministry did advise that the ITP Program offers training as it pertains to searching, whether that is property entering the Centre or supplies entering the unit. The ITP also speaks to the importance of confidentiality of inmate files, ensuring that what is contained in it is secured and not accessible to inmates or others not authorized to view or have access to the file. This was included in the ITP Program when the CO completed the training.

[60] Although it appears the CO did not have specific privacy training, I am satisfied that they were provided with training that made them fully aware of their obligations including that they are not to leave an inmate file inside of a food cart, and must search any item (including food carts) upon entering the unit.

[61] I commend the Ministry for now including access and privacy training as part of the ITP for CO's.

[62] In addition, the Ministry advised as of December 2018 all correctional centre staff are required to complete the online access and privacy training, with the completion of the training being monitored by their supervisors.

[63] These are great steps for the Ministry. However, so that the importance of protection of privacy is not lost through the passage of time, it is crucial for staff to be given privacy training refreshers on an annual basis. These refreshers can range from formalized training, such as completing the online training each year, to less formal by having discussions about privacy obligations at staff meetings. Whatever the method of delivery, the Ministry should require that staff complete privacy refresher training on an annual basis, tracking that the employee has completed the training and recording it in the employee's personnel file.

[64] Based upon the Ministry's investigation of this matter, it appears the CO was given the appropriate training to know that all items must be searched upon entering the unit. Therefore, I conclude that the root cause of this breach of privacy was negligence on the part of the CO. Had the CO not been negligent, the inmates would not have been able to view and take a portion of the file and the assault resulting in death may not have occurred.

[65] I find the Ministry conducted an adequate privacy investigation.

Step 4: Prevent Future Breaches

[66] An important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. When considering what changes should be made, the public body can ask itself the following questions:

- 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?

[67] The Ministry has acknowledged that there was no effort by the CO to contain the breach, take steps to mitigate potential harm to the affected individual or notify the appropriate officials of the matter.

[68] The Ministry also advised that the Saskatchewan Public Service Commission was engaged to review and advise on the matter. The Ministry advised my office that the employee was on leave, but would not disclose to my office whether the leave was related to disciplinary action or was a personal leave. In follow-up communications with the Ministry in December 2019, they advised that the CO's employment was terminated. However, when responding to my draft report, the Ministry advised that the employee went through the grievance process and as a result, has now regained employment at an alternate location in the Ministry.

[69] The Ministry advised that during the privacy investigation, the SCC began to take steps to reduce the risk of a similar occurrence happening in the future. The SCC sent correspondence to all employees outlining their protection of privacy obligations to ensure confidentiality and security of offender files, with increased attention to immediately report any potential privacy breaches to their supervisor. In addition the SCC's search policy has been amended to include specific language respecting searching of food carts.

[70] The Ministry should go a step further to mitigate the risk of this happening in the future. By multitasking duties such as food cart and inmate file transportation, there is a risk of this type of breach happening in the future. Therefore, the Ministry should develop a new policy that explicitly states that the transporting of inmate files or files containing personal information and/or personal health information cannot occur at the same time as other duties. In short, transporting inmate files should be a stand alone duty.

[71] I am satisfied the Ministry has taken adequate steps to mitigate this happening again in the future. However, in order for staff to be fully aware of their obligations and the policies and procedures they must follow, awareness, training and procedural reminders should continue on an ongoing basis.

[72] I find the Ministry took adequate steps to prevent the risk of this type of breach of privacy occurring in the future.

Step 5: Privacy Breach Report

[73] Once the necessary information has been collected, it is a good practice to prepare a privacy breach investigation report. The report should include the following:

- A summary of the incident and immediate steps taken to contain the breach.
- Background of the incident. Timelines and a chronology of events.
- Description of the personal information involved and the affected individuals.
- A description of the investigative process.
- The root and contributing causes of the incident.
- A review of applicable legislation, safeguards, policies and procedures.
- A summary of possible solutions and recommendations for preventing future breaches, including specific timelines and responsibility for implementation of each action.

[74] The Ministry provided my office with its investigation report, including supporting documentation, on August 14, 2018. My office continued work on this file once both sentencing hearings concluded. In December 2019, the Ministry answered additional questions my office had surrounding its investigation.

[75] The Ministry addressed the necessary information required in its investigation report to enable my office to conduct our investigation.

[76] Therefore, I find the Ministry prepared an adequate privacy breach report.

[77] This truly is the worst case scenario that can happen as a result of a privacy breach. My hope is that through this tragedy everyone, including staff of correctional facilities, can learn from this and that it really solidifies why protection of privacy obligations and the duty to protect that information is critical.

[78] I would also like to extend my sympathies to the family and friends of the Deceased Individual.

III FINDINGS

[79] I find a privacy breach occurred.

[80] I find the Ministry did not contain this breach of privacy.

[81] I find the Ministry's notification efforts to be insufficient as the Deceased Individual was not notified that the file was in the possession of another inmate for a period of time.

[82] I find the Ministry conducted an adequate privacy investigation.

[83] I find the Ministry took adequate steps to prevent the risk of this type of breach of privacy occurring in the future.

[84] I find the Ministry prepared an adequate privacy breach report.

IV RECOMMENDATIONS

[85] I recommend the Ministry consider the incident response steps I have outlined in paragraph [23] to determine if they are appropriate to add to incident responses of privacy breaches involving inmates.

[86] I recommend the Ministry implement a notification process to inmates where their privacy has or may have been breached.

[87] I recommend the Ministry implement a policy change that requires the transporting of inmate files, or any other record containing personal information and/or personal health information of inmates is a stand alone practice and not to be combined with other CO job duties.

[88] I recommend that the Ministry provide the Deceased Individual's next of kin a copy of my investigation report.

[89] I recommend that correctional centre staff sign the Oath on an annual basis.

[90] I recommend the Ministry amend the Oath to include reference to HIPA.

[91] I recommend the Ministry amend the Oath to include employee's duty to protect obligations pursuant to sections 24.1 of FOIP and 16 of HIPA.

[92] I recommend the Ministry amend the Code to include employees' duty to protect obligations pursuant to sections 24.1 of FOIP and 16 of HIPA.

[93] I recommend the Ministry amend the Code so that all staff are required to review and specifically sign the Code on an annual basis.

[94] I recommend the Ministry require that correctional centre staff complete mandatory annual refresher privacy training, and track completion for each staff member.

Dated at Regina, in the Province of Saskatchewan, this 7th day of May, 2020.

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