Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 319-2017

Ministry of Corrections and Policing

June 1, 2018

Summary: The Ministry of Corrections and Policing (Corrections) undertook an investigation into 22 missing probation files. The Commissioner found that, overall, Corrections responded appropriately to the breach. He noted that, given the sensitive nature of the personal information and personal health information, Corrections should have expedited the investigation and the notification of affected individuals. He also recommended that Corrections amend its *Code of Professional Conduct* to include more specific language about the protection of personal information and personal health information. He also recommended that Corrections forward its investigation file to the Ministry of Justice and Attorney General, Public Prosecutions Division to determine whether an offence has occurred and whether charges should be laid under FOIP

I BACKGROUND

[1] At the time of the privacy breaches, the Ministry of Justice was a single ministry. However, during the course of this review, the Ministry of Justice was split into two ministries: the Ministry of Justice and Attorney General and the Ministry of Corrections and Policing. My office has been advised that the privacy breach involved personal information and personal health information in branches that would now fall under the Ministry of Corrections and Policing. Therefore, this report will refer to Corrections and Policing.

[2] On December 11, 2017, the Ministry of Policing and Corrections (Corrections), proactively reported a privacy breach to my office. It advised that 11 probation physical files had gone missing. Nine of the files were missing from the North Region and two from the South Region. Through the course of its investigation, it discovered an additional 11 missing physical files.

[3] My office notified Corrections that we would undertake an investigation on December 12, 2017.

II DISCUSSION OF THE ISSUES

1. Does FOIP apply in these circumstances?

[4] *The Freedom of Information and Protection of Privacy Act* (FOIP) applies to privacy matters when three elements are present. The first element is a government institution, the second element is personal information and the third element is if the personal information is in the possession or control of the government institution.

[5] Corrections qualifies as a government institution pursuant to subsection 2(1)(d)(i) of FOIP which provides:

> 2(1) In this Act:
> …
> (d) "government institution" means, subject to subsection (2):
>
> (i) the office of Executive Council or any department, secretariat or other similar agency of the executive government of Saskatchewan; or

[6] Subsection 24(1) of FOIP defines personal information. The relevant portions are as follows:

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

> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> (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;
> …
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
>
> (e) the home or business address, home or business telephone number or fingerprints of the individual;
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
>
> (ii) the disclosure of the name itself would reveal personal information about the individual.

[7] The personal information involved in this privacy breach is that found in the probation files of 22 individuals. Specific data elements typically include identifying information (date of birth, address and physical description). The files have information about the individual's family and marital status. The files in question also contain personal information relating to the individuals' criminal history such as warrant reports, criminal history reports, risk assessments, program applications and reports, case management plans and notes, presentence reports, bail reports and breach/violation reports. This information qualifies as personal information pursuant to subsections 24(1)(a), (b), (d), (e) and (k) of FOIP.

[8] The personal information was in the possession and control of Corrections at the time of the breach.

2. Does HIPA apply in these circumstances?

[9] *The Health Information Protection Act* (HIPA) applies to privacy matters when three elements are present. The first element is a trustee, the second element is personal health information and the third element is if the personal health information is in the custody or control of the trustee.

[10] Corrections qualifies as a trustee pursuant to subsection 2(t)(i) of HIPA which provides:

> 2 In this Act:
> …
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> (i) a government institution;

[11] Corrections indicated that there can also be information about individuals' mental health and addictions in these files. This would qualify as personal health information pursuant to subsection 2(m)(i) 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;

[12] The personal health information was in the custody and control of Corrections at the time of the breach.

3. Did Corrections respond appropriately to this privacy breach?

[13] In circumstances where there is no dispute that a privacy breach has occurred, the focus for my office becomes one of determining whether the trustee has appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that Corrections took the privacy breach seriously and appropriately addressed it. In multiple

resources, my office recommends five best practice steps be taken by a government institution or trustee when responding to privacy breaches. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Plan for prevention; and
5. Write a privacy breach report.

[14] I will use these steps to assess Corrections' response to the breach.

Contain the Breach

[15] Upon learning that a privacy breach has occurred, trustees 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.

[16] Corrections reported that, between 2016 and 2018, 22 probations files were missing. The first was reported in September 2016. The next 10 missing files were reported throughout 2017. The final 11 were discovered missing during Corrections' investigation.

[17] Each time the first 11 files were discovered missing, Corrections searched for the files. It kept a detailed account of each search. However, only one file was recovered.

[18] Corrections indicated that after the first file went missing in September 2016 it launched an investigation. The investigation has lasted more than 15 months. During that time, 10 more files were reported missing. Corrections did not proactively report the missing files to my office until 15 months after the first missing file was reported. It discovered that 11 additional files were missing 16 months after it launched its investigation. I recommend that Corrections expedite investigations, especially those that involve particularly sensitive and prejudicial personal information and personal health information such as criminal history and mental health information.

Notify affected individuals and/or appropriate organizations

[19] Notifying an individual that their personal information and/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, government institutions and trustees should always notify affected individuals.

[20] Corrections has made reasonable efforts to notify all affected individuals, but could not locate all of them. I note that Corrections indicated that notifications were underway in January 2018, which was 16 months after the first file was reported missing.

[21] My office has always indicated that it is best practice to notify affected individuals of a breach involving their personal information or personal health information. This is particularly necessary when the breach involves sensitive personal information or personal health information. Affected individuals need to be alerted so they can protect themselves from any potential harm. In this case, the information in question contained sensitive personal information and personal health information including criminal history and mental health information which carry stigma and can cause prejudice. Further, the fact that the information is missing could impact future interactions between the affected individuals and the justice system.

[22] I note that on January 1, 2018 a new amendment to FOIP came into effect which provides:

> 29.1 A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[23] The federal *Personal Information and Electronic Documents Act* (PIPEDA) defines 'significant harm' as bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. Corrections does

not know what happened to the files so there is likely a real risk that there could be harm as a result of the loss of these files.

[24] Although this provision was not in effect throughout the majority of Correction's investigation, it signifies that there was an urgent need to provide notification. Corrections noted that it worked to establish a cohesive and coordinated action plan to report missing files and to notify the affected individuals. In my view it is simple to write a letter to an affected individual and it should have occurred immediately after a thorough search had taken place for each missing file.

[25] In the future, I recommend Corrections provide notification to affected individuals shortly after the effected individual's file is found to be missing.

[26] Corrections also proactively reported the breach to my office.

Investigate the breach

[27] Once the breach has been contained and appropriate notification has occurred, the government institution or trustee should conduct an internal investigation. The investigation is generally conducted by the public body's access and privacy unit 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 systemic basis and should include a root cause analysis. It should also consider whether the safeguards that were in place at the time of the incident were adequate. The investigation should be documented in an internal privacy breach investigation report. At the conclusion of its investigation, the public body should have a solid grasp on what occurred.

[28] Corrections was alerted to 10 of the first 11 files when inactive files were reactivated. When Corrections staff went to retrieve the files, it was discovered that they were missing. This occurred on various dates in 2016 and 2017. The last of the first missing 11 files was identified because the case was still active. It was missing one of two volumes of physical files. In May 2018, Corrections located this file.

[29] When each of the first 11 files went missing, Corrections searched thoroughly for the records. Further, when it discovered that 11 additional files had gone missing during the investigation, Corrections also searched for these files. This included reviewing logs (deadwood, file transfer and Gemini), probation officers assigned, location, CVA vehicles and interviewing staff. Corrections kept a detailed record of the search for each record.

[30] Other techniques that Corrections used to investigate the matter included a file audit, interviewing staff, reviewing procedures and other existing safeguards.

[31] Corrections noted that 16 of the 22 files belonged to one probation officer. However, the interviews with that probation officer did not shed any light on what may have happened to the files. The probation officer has since been terminated. No charges have been laid pursuant to FOIP against the former probation officer at this time.

[32] 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.

[33] As of January 1, 2018, 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.

[34] I note that subsection 24.1 of FOIP was not in place at the time that the files were discovered missing, however, my office has always said that government institutions have a duty to protect personal information.

[35] Corrections reported that there are over 8000 active probation files each year. The probation files remain with designated probation officers until the case is closed. They are then provided to a supervisor for sign off. The files then sit in "deadwood" for six years. At that time, they are transferred to Gemini for permanent storage. All but one of the missing files were inactive and supposed to be in deadwood in their respective offices.

[36] Corrections has listed the following safeguards that were in place:

Physical Safeguards

- Physical Probation files are stored in a locked file cabinet in locked offices or locked file room.
- Removal of files for court, case conferences and other reasons are approved by the director and must be transported in a secure manner (locked briefcase or bag).
- Both are enshrined in a written policy.

Technical Safeguards

- A paper file and electronic file are created for each offender. However, the files do not always contain the same information. Personal information would be lost from the paper files.

- Electronic files are stored within the secured offender management system (Criminal Justice Information Management System (CJIMS)).

- All files (Probation Officer assignment of probation client files and transfers amongst the Community Corrections offices) are managed and tracked through CJIMS.

- Tracking logs:

    - Transfer log – tracks all file transfers between Community Corrections Offices (trace mail slips and excel database);
    - Deadwood Log – tracks files placed in and removed from on-site deadwood;
    - Records Transfer Log – tracks files transferred to and from Gemini, and Disposal Year.

Administrative Safeguards

- The *Oath or Declaration of Office* form which all Corrections employees sign upon employment.

- *Code of Professional Conduct* reviewed and signed annually by all Corrections employees. Includes provisions for 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. This document only refers to personal information of employees in a specific manner.

- CSRS Policies:

    - "Disclosure of information", Custody Services, Administration 0007 and Security 0024, last updated June 2016. This policy pertains to the collection, use and disclosure of PI and PHI, there is no reference to the physical security of paper files;

    - "Maintenance and Use of Records" Community Corrections, Administration 09, last updated August 2017. This policy, specifically, section 3.1 to 3.6 speaks to how and when to report a missing file and to whom within specific guidelines and timelines;

    - Ministry of Justice Records Management Guides
        - How do I Dispose of Records
        - How do I Permanently Remove box-file From a Transfer
        - How do I Process a New Transfer
        - How do I Recall a Box from the Records Centre
        - How do I Send Records to the Records Centre.

- Privacy and Access Training:
    - All CSRS staff complete the Saskatchewan Government's Access and Privacy self-directed learning module.

[37] I note that the *Oath or Declaration of Office*, which appears in *The Public Service Regulations, 1999* explicitly indicates that employees must comply with FOIP and HIPA; however, it does not specifically mention the protection of personal information or personal health information. In addition, the *Code of Professional Conduct* is not explicit with respect to the protection of personal information and personal health information. It states:

> 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. There may be times when information sharing is appropriate and required as a part of an employee's duties. If unsure, employees should contact their supervisor for clarification.

[38] In my view, this passage in the *Code of Professional Conduct* and the *Oath or Declaration of Office* are not explicit enough to signal to employees that it is important and necessary to protect personal information and personal health information. Further, the document lists FOIP as an authority for which the code was written, however, it does not mention HIPA. Best practice is that government institutions and trustees require that employees sign a confidentiality agreement on an annual basis. I recommend that Correction amend its *Code of Professional Conduct* to include more explicit and specific language about the protection of personal information and personal health information.

[39] Only one of the missing records were not recovered. As such it is difficult to say for certain what caused each breach. As mentioned, the investigation lasted 16 months. An expedited investigation might have resulted in better results and prevented subsequent missing files. Therefore, in this investigation, there are various causes for breaches. In one case, a file was removed from Gemini without following the proper procedure. Therefore, employees not following proper procedures is one cause. In another case, an active file was missing. In many cases, files were meant to be in deadwood, but were not found there. There was no written procedure or tracking system in place in these cases.

Plan for prevention

[40] The next step is to formulate a plan to avoid future breaches of a similar nature. Some changes that are needed may have revealed themselves to the public body during the investigation phase, such as deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training. This is an important step in addressing a privacy breach because a privacy breach cannot be undone but the public body can learn from it and improve.

[41] Corrections reported the following steps in its plan for prevention:

- A tracking process was put in place in an office in La Ronge in February 2017. Corrections will expand it to all Community Corrections offices to ensure a practice is in place to manage and track the Probation files within the branch.

- Corrections will review current internal file movement and transfer practices and transfer logs and consider establishing standardized internal processes and templates.

- Corrections will follow up with the individuals responsible for the missing files at the conclusion of the investigation. This will include requiring individuals to review the *Maintenance and Use of Records* policy.

- All Community Corrections staff were reminded of the updated *Maintenance and Use of Records* policy.

- Remind all administrative staff of the record transfer to Gemini process.

- Identify access and privacy and records management training needs and develop plan for Community Corrections.

- Documentation of this matter was placed on the individuals responsible for the missing files personnel files.

Write a privacy breach report

[42] Corrections has created a detailed privacy breach report.

III FINDING

[43] I find that, although the investigation took many months to complete, Corrections responded appropriately to the breach.

IV RECOMMENDATIONS

[44] I recommend that Corrections continue with its plan for prevention.

[45] I recommend that Corrections ensure timely investigations of privacy breaches which include notifying affected individuals as soon as possible.

[46] I recommend Corrections amend its *Code of Professional Conduct* to include explicit language about protecting personal information and personal health information.

[47] I recommend that Corrections forward its investigation file to the Ministry of Justice and Attorney General, Public Prosecutions Division to determine whether an offence has occurred and whether charges should be laid under FOIP.

Dated at Regina, in the Province of Saskatchewan, this 1st day of June, 2018.

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