Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 088-2022

Ministry of Corrections, Policing and Public Safety

October 21, 2022

Summary: The Complainant made a complaint about a privacy breach involving the Ministry of Corrections, Policing and Public Safety (Corrections). A Corrections' employee had inappropriately accessed the Complainant's information. Corrections notified the Complainant who was not satisfied with Corrections' response to the breach. The Commissioner investigated the incident and found that a privacy breach had occurred. The Commissioner also found that Corrections' notice to the Complainant was not adequate, and it did not take adequate steps to contain and investigate the breach. The Commissioner however found that Corrections' plan to prevent further breaches was adequate. The Commissioner recommended Corrections amend its breach containment and investigation practices. The Commissioner also recommended that Corrections report back to his office on completion of its plan to prevent further breaches.

I BACKGROUND

[1] On May 16, 2022, the Complainant asked my office to investigate a privacy breach involving the Ministry of Corrections, Policing and Public Safety (Corrections). Corrections had informed them of the breach by letter dated May 9, 2022. The letter stated that a Corrections' employee had accessed their personal information without authorization on five occasions. The unauthorized accesses occurred between May 13, 2021, and January 7, 2022.

[2] On May 24, 2022, my office notified Corrections of our intention to investigate the breach pursuant to section 33 of *The Freedom of Information and Protection of Privacy Act*

(FOIP). We requested that Corrections complete the *Privacy Breach Investigation Questionnaire*.

[3] On July 25, 2022, Corrections provided my office with its Privacy Incident Internal Investigation Report (Corrections' report). Corrections' report acknowledged that a privacy breach occurred involving unauthorized accesses. It clarified that its employee accessed the Complainant's file on four occasions, and not five.

[4] The Complainant's information was stored in the Criminal Justice Information Management System (CJIMS). Their information included the Complainant's name, date of birth, gender, address, photograph, information about their criminal history. Corrections was not able to confirm that the Complainant's Driver's License Number (DL) had been accessed. It stated that the DL was stored in the "Courts" portions of the CJIM file, as opposed to the "Corrections" portion.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[5] The privacy rules in FOIP apply to personal information in the possession or control of government institutions. Corrections qualifies as a "government institution" as defined in subsection 2(1)(d)(i) of FOIP which states:

> **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;

[6] Corrections asserted that the information accessed by its employee was personal information. I agree. The Complainant's name, date of birth, gender, address, photograph, and information about their criminal history qualify as personal information under

subsections 24(1)(a), (b), (e) and (k)(i) of FOIP. The Complainant's DL would qualify as personal information under subsection 24(1)(d) of FOIP.

[7] Subsections 24(1)(a), (b), (d), (e), and (k)(i) of FOIP state, in part:

> **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, color, 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

[8] As Corrections is a government institution and this breach involved personal information, I find that I have jurisdiction to investigate this matter under FOIP.

2. Did a privacy breach occur?

[9] When a government institution collects, uses or discloses "personal information" without authority a privacy breach occurs. I have already found that this breach involved personal information. Therefore, to determine if a privacy breach occurred, I must also decide if there was an unauthorized collection, use, or disclosure of that personal information.

[10] A "use" of personal information includes reference to or manipulation of personal information (Investigation Report 040-2021). I find that the accesses to the Complainant's personal information in this case were uses.

[11] FOIP requires that uses of personal information be based on the need-to-know principle. Need-to-know requires a government institution to only use personal information where it is necessary to do so. This means that government institutions should only use personal information where there is a legitimate need to know for the purpose of delivering their mandated services. This approach is consistent with previous reports of my office, such as Investigation Reports 234-2020 and 278-2017.

[12] Corrections asserted that its employee had not been assigned to the Complainant's file. Therefore, they had no work-related purpose to access it and their use did not comply with FOIP. Based on this information, I find that the employee's use did not comply with FOIP and a privacy breach under FOIP occurred.

3. Did Corrections respond appropriately to the privacy breach?

[13] As set out in my office's Rules of Procedure, when we determine that there has been a privacy breach, we will analyze whether the government institution appropriately managed the breach. We will also consider if it:

- Contained the breach (as soon as possible)
- Notified affected individuals (as soon as possible)
- Investigated the breach
- Took appropriate steps to prevent future breaches.

[14] I turn to consider if Corrections followed these steps.

Contained the breach (as soon as possible)

[15] Upon learning that a privacy breach has occurred, government institutions should immediately take steps to contain the breach to reduce its impact. 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 to personal health information
- Correcting weaknesses in physical security

(*Privacy Breach Guidelines for Government Institutions and Local Authorities*, August 2022 at p. 4)

[16] The circumstances of this breach and its containment were as follows:

January 25, 2022 – Corrections received information about a possible conflict of interest on the part of the employee from another Corrections' employee. Corrections started a workplace investigation into the allegation

March 17, 2022 – As part of its investigation into a possible conflict of interest, Corrections interviewed the employee who admitted that they had accessed the Complainant's CJIMS file for non-work-related reasons

March 30, 2022 – Corrections placed the employee on administrative leave and took away their right to access CJIMS

April 5, 2022 – Corrections conducted an audit of CJIMS and confirmed the unauthorized accesses

April 13, 2022 – Corrections interviewed the employee who confirmed the unauthorized accesses

April 20, 2022 – Corrections advised its Privacy Unit of the breach

May 2, 2022 – Corrections terminated the employee's position

May 9, 2022 – Corrections notified the Complainant of the breach.

[17] It took Corrections two weeks after learning of the unauthorized access to terminate the employee's access rights. It took over two weeks to conduct the audit of CJIMS. Corrections waited over one month before it notified its Privacy Unit of the breach.

[18] Given the allegations of a potential conflict of interest, Corrections' staff should have advised the Privacy Unit at the earliest opportunity. The privacy staff have the expertise to identify and respond to privacy breaches. Corrections should also have conducted an audit of CJIMS as soon as it was aware that an employee with access to that system was involved in allegations of workplace misconduct.

[19] In this case, it appears there were no unauthorized accesses between the date the allegations were made and the date of the audit. Therefore, no harm resulted from Corrections' delay. However, the delay in conducting the audit, terminating the employee's access rights, and advising Corrections' Privacy Unit was not consistent with best practices which require containment efforts to occur as soon as possible. Therefore, I find that Corrections' efforts to contain the breach were not adequate.

[20] I recommend that Corrections' staff notify its Privacy Unit at the earliest opportunity after becoming aware of a risk of inappropriate behaviour that could involve personal information. Corrections should also conduct audits of information systems at the earliest opportunity after becoming aware of a risk of inappropriate behaviour that could involve personal information.

Notified affected individuals (as soon as possible)

[21] Section 29.1 of FOIP requires that, if there was an unauthorized use or disclosure of personal information, government institutions notify the affected individual(s) where the "incident creates a real risk of significant harm" (*Privacy Breach Guidelines for Government Institutions and Local Authorities*, p. 4).

[22] Section 29.1 of FOIP states:

> **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] Even where section 29.1 of FOIP does not apply, unless there is a compelling reason not to, government institutions should always notify affected individuals of a privacy breach.

[24] It is important to notify affected individuals for several reasons. Affected individuals have a right and need to know to protect themselves from any harm that may result. Government institutions may also want to notify organizations, such as, my office, law enforcement or other regulatory bodies that oversee professions.

[25] A notice to affected individual(s) should include:

- A general description of what happened
- A description of the personal information involved (e.g., name, date of birth, etc.)
- A description of the types of harm that may result because of the privacy breach
- Steps taken and planned to mitigate the harm and to prevent future breaches
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves
- Contact information of an individual within the organization who can answer questions and provide information
- A notice that individuals have a right to complain to the IPC
- Recognition of the impacts of the breach on affected individuals and an apology

(*Privacy Breach Guidelines for Government Institutions and Local Authorities*, p. 6)

[26] Corrections did not notify my office of this breach. It notified the Complainant on May 9, 2022. The notice included a description of the privacy breach and a statement that steps had been taken to ensure no further unauthorized access by the employee. It also included an apology, Corrections' contact details and notice about the right to complain to my office.

[27] The notice did not include a description of the personal information involved, the steps taken to mitigate the risk and prevent future breaches. Also, it did not include a description of the types of harm that might result from the breach and advice on how to protect against further harm.

[28] With respect to the description of the personal information, Corrections asserted that information on a CJIMS screen is "dynamic" and may change from time to time. After providing the initial notice, it sent a letter dated August 8, 2022, to the Complainant listing the personal information typically included on the CJIMS screens accessed by the employee.

[29] Corrections also asserted that the steps taken to contain and mitigate the risks of harm were set out in the August 8, 2022, letter and verbally explained to the Complainant. However, the letter only states that Corrections has taken steps to ensure that the employee can no longer access the personal information. The letter does not mention that Corrections had terminated the employee's employment.

[30] I appreciate that the August 8, 2022, letter may have provided additional information about the breach. Corrections may also have provided some additional information verbally. However, the information described above should have been provided to the Complainant at the earliest opportunity – not over four months after discovery of the breach.

[31] Corrections should ensure its breach notices include more detail about the personal information involved, the nature of the privacy breaches and the steps taken to mitigate risks. It not only assists affected individuals, but it ensures Corrections is considering the risks and impacts of all breaches.

[32] Corrections should also have informed the Complainant of any disciplinary measures taken against the snooping employee. It is not enough to state that the employee's access rights were terminated (Investigation Report 088/2013, Investigation Report 136-2017, *Privacy Breach Guidelines for Government Institutions and Local Authorities*, p. 8).

[33] For the reasons set out above, I find that Corrections' notice to the Complainant was not adequate. I recommend that Corrections review its notification practices and ensure that, in the future, it meets the requirements set out in my office's *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

Investigated the breach

[34] After containing the breach and notifying affected parties, government institutions should conduct an internal investigation. The investigation should address the incident on a systemic basis and should include a root cause analysis. At the conclusion of its investigation, they should understand the cause of the breach which will inform how to prevent future breaches.

[35] Once Corrections' Privacy Unit received notice of the breach on April 20, 2022, it interviewed two Directors involved in the workplace investigation. It also completed a review of the following documents:

- Notes from three fact-finding interviews with the employee
- Request for Access to CJIMS form, signed by the employee
- CJIMS Authorized Access, Use and Restrictions Policy
- Codes of Professional Conduct, signed by the employee

[36] The Privacy Unit could not interview the employee because by the time that it received notice of the breach, Corrections had terminated the employee's employment.

[37] Corrections' Privacy Unit's investigation included a review of privacy safeguards that were in place and concluded that they were adequate. It asserted:

- Physical tokens are required for all CJIMS users
- CJIMS uses multi-factor authentication based on a user password, random code generated by physical token and security clearance screening
- An on-screen pop-up banner is used to alert staff on appropriate use of the system when they log into CJIMS
- Training on privacy and acceptable use of CJIMS is provided
- Oath of Office and CJIMS Request for Access Agreements include information about appropriate use and disclosure of personal information

[38] Corrections' report concluded that the privacy breach was a result of the failure of its employee to comply with policy. It also concluded that it could not have avoided the breach.

[39] I agree with Corrections that one of the causes of this breach was a failure of Corrections' employee to comply with existing policy. However, I disagree with Corrections' conclusion that it could not have avoided this privacy breach. If Corrections had in place a program of regular random audits of CJIMS and made its users aware of the program, it might have avoided the breach.

[40] I also note that Corrections could have avoided the breach if it had limited the employee's CJIMS access rights to the information required to provide services to their clients. Access controls that limit access rights based on a need-to-know are called role-based access controls. They are one of the best ways to limit who has access to what information in an information system (Office of the Privacy Commissioner of Canada, Office of the Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner of British Columbia, *Getting Accountability Right with a Privacy Management Program*, April 2012).

[41] Corrections' report included recommendations to implement a program of random auditing and role-based access controls. I will discuss this further below.

[42] For the same reasons that I have found that Corrections' containment was not adequate, I find that Corrections' investigation into the privacy breach was not adequate. Corrections should have involved its Privacy Unit staff and conducted an audit of CJIMS at the earliest opportunity.

Took appropriate steps to prevent future breaches

[43] Prevention is one of the most important steps. A privacy breach cannot be undone but a government institution can learn from one and take steps to help ensure that it does not

happen in the future. To avoid future breaches, government institutions should make a prevention plan.

[44] As noted above, Corrections' report included recommendations about steps it could take to prevent future breaches. Corrections subsequently prepared a workplan setting out the proposed actions. The relevant recommendations, proposed actions and completion target dates are set out in the following table:

Number	Recommendation	Proposed Action	Completion Target Date
1	Review current practices to determine where gaps may exist in policies, procedures, and/or training.	Review Provincial Policy **Information Management 902 -** *Criminal Justice Information Management System (CJIMS) Authorized Access, Use and Restrictions* and determine if there needs to be updates to meet the following recommendations.	October 31, 2022
2	Develop additional policy and/or training that addresses the penalties associated with snooping in CJIMS and informs employees of their duty to protect personal information under FOIP and personal health information under HIPA.	Review Provincial Policy **Information Management 902 -** *CJIMS Authorized Access, Use and Restrictions* and determine if there needs to be updates to meet the following recommendations. The Audit, Information Management and Safety, Integrated Justice Services (IJS) has developed a refresher privacy course for the Ministry that will be available by the end of the fiscal year.	October 31, 2022 March 31, 2023
3	Develop and use a standard script when new employees sign the *CJIMS Request for Access* form to ensure they understand improper uses of CJIMS.	Continue to ensure that **employees** are reviewing and signing the access form. The request for access form will be updated with the new policy. It contains the following script: **Inappropriate Use of CJIMS:** CJIMS must not be used for activities contrary to the *CJIMS Authorized Access, Use and*	October 31, 2022

		Restrictions policy or the law, such as to search or use information on any person(s) for personal reasons (snooping), to conduct unauthorized research data or reports or for any reason other than ministry business, legislative requirements, or approved lawful purposes. Inappropriate use of CJIMS may be reported to, and access and usage may be audited by, the CJIMS Authority or the Information and Privacy Officer. Any violation of provincial policy may be investigated, prosecuted under the *Criminal Code of Canada* and may result in corrective discipline, up to and including dismissal.	
4	Periodically review the Provincial Policy **Information Management 902 -** *CJIMS Authorized Access, Use and Restrictions* policy with employees to ensure understanding and compliance.	The annual refresher of the *Ministry of Corrections, Policing and Public Safety Professional Code of Conduct* outlines employee's responsibility at not disclosing information and protecting information. The Provincial Policy – **Information Management 902** will be emailed to all Community Corrections employees by the Director of Regions annually as part of the refresher.	October 31, 2022
5	Implement a random sampling/audit schedule for CJIMS users. Assign a resource to manage this function to ensure it is regularly completed.	The Audit, Information Management and Safety Branch, IJS, will work with the Strategic Systems and Innovation Branch within Corrections, Policing and Public Safety to explore CJIMS's audit functions.	March 31, 2023
6	Develop an online refresher training course for employees to re-familiarize themselves with the obligations surrounding acceptable	The Audit, Information Management and Safety Branch, IJS has developed a refresher privacy course for the ministry that will be available by the end of the fiscal year.	March 31, 2023

	and unacceptable use of personal information in CJIMS.		
7	Ensure employees complete a Declaration of Conflict of Interest when they engage in employment outside of government.	Mandatory Training - Employees have been advised they all need to complete the online LEARN module of Government of Saskatchewan's Corporate Conflict of Interest Training by April 30, 2023. Government of Saskatchewan has an updated policy effective April 11, 2022.	April 30, 2023
8	Limit an employee's CJIMS access to only the records/clients necessary to perform their job duties.	The Audit, Information Management and Safety Branch, IJS, will work with the Strategic Systems and Innovation Branch within Corrections, Policing and Public Safety to examine CJIMS's role-based access controls.	March 31, 2023

[45] I agree with Corrections' recommendations. Subject to the comments below, I recommend that Corrections comply with the proposed actions and report back to my office on the results by the completion target date.

[46] Corrections' recommendation number two should include a requirement to inform all staff of the disciplinary action taken against the employee for snooping. Corrections should inform its staff of specific examples of privacy breaches that have occurred within the organization and of the discipline that followed. Repeatedly reminding employees that there is no tolerance for unauthorized access to personal information and personal health information can deter and prevent privacy breaches.

[47] Recommendation number five is about implementing a random audit program. Auditing is a technical safeguard and is necessary to assess compliance with policies, procedures, and legislation. With respect to random audits, my office's *Auditing and Monitoring Guidelines for Trustees*, which also apply to government institutions, states:

> Random audits should be used by the trustee to ensure user compliance with provincial and federal legislation, joint services and access policies [] and with the trustee's internal privacy and security policies. It is the trustee's responsibility to establish a process for conducting random audits of user activity.

[48] Random audits are an important measure to protect privacy of personal information and personal health information. Managed properly random audits can be effective in detecting and deterring privacy breaches. Further information about implementing a random audit program is in the guidelines referred to above. In addition to implementing recommendation number five, Corrections should ensure that the program is transparent. It should advise staff about the program and the fact that it will occur without notice to employees.

[49] I find that Corrections has developed a good plan to prevent further breaches. I recommend that it consider the additional recommendations made in paragraphs [46] and [48] above.

III FINDINGS

[50] I find that I have jurisdiction to investigate this matter.

[51] I find that a privacy breach occurred.

[52] I find that Corrections' efforts to contain the privacy breach were not adequate.

[53] I find that Corrections' notification to the Complainant was not adequate.

[54] I find that Corrections' investigation of the privacy breach was not adequate.

[55] I find that Corrections' plan to prevent further breaches was adequate.

IV RECOMMENDATIONS

[56] I recommend that Corrections' staff notify its Privacy Unit at the earliest opportunity after becoming aware of a risk of inappropriate behaviour that could involve personal information. Corrections should also conduct audits of information systems at the earliest opportunity after becoming aware of a risk of inappropriate behaviour that could involve personal information.

[57] I recommend that Corrections review its notification practices and ensure that, in the future, it meets the requirements set out in my office's *Privacy Breach Guidelines for Government Institutions and Local Authorities*.

[58] I recommend that Corrections comply with the proposed actions described in paragraph [44], subject to the additional recommendations made in paragraphs [46] and [48] above.

[59] I recommend that Corrections report back to my office on its compliance with paragraphs [56] and [57] within 30 days of the date of this Report.

[60] I recommend that Corrections report back to my office on its compliance with paragraph [58] by the completion target dates set out in paragraph [44].

Dated at Regina, in the Province of Saskatchewan, this 21st day of October 2022.

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