Office of the
Saskatchewan Information
and Privacy Commissioner

# INVESTIGATION REPORT 110-2019

## Ministry of Corrections, Policing and Public Safety

**January 7, 2021**

**Summary:** The Ministry of Corrections and Policing and Public Safety (Corrections) received an alleged breach of privacy complaint related to the collection and use of the Complainant's personal health information. Corrections responded to the Complainant indicating that a breach had occurred in one instance. The Commissioner investigated the complaint and found that further breaches occurred and that Corrections had not responded to the breach appropriately. The Commissioner recommended that Corrections contain the breach, develop appropriate procedures to ensure that this type of breach does not occur again and issue an apology to the Complainant.

## I BACKGROUND

[1] On February 10, 2019, the Complainant advised the Ministry of Corrections and Policing that their privacy was breached when the Ministries' staff members allegedly accessed the Complainant's personal health information without consent. Since the complaint was made, the official name of the Ministry has been changed to the Ministry of Corrections, Policing and Public Safety (Corrections).

[2] On March 25, 2019, Corrections responded to the Complainant, confirming the Complainant's privacy had been breached by one staff member (Director 1), but not the other (Director 2).

[3] On April 10, 2019, the Complainant reported to my office that they were not satisfied with the outcome of Corrections' investigation into their privacy complaint.

[4] On April 15, 2019, my office informed both the Complainant and Corrections of its intention to investigate the matter.

## II DISCUSSION OF THE ISSUES

### 1. Is *The Health Information Protection Act* (HIPA) engaged?

[5] HIPA is engaged when three elements are present: 1) personal health information, 2) a trustee, and 3) personal health information is in the custody or control of the trustee.

[6] First, subsection 2(m) of HIPA defines personal health information as follows:

> **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 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;

[7] The Complainant's personal health information was contained in a physician's report titled, *Confidential Physician Assessment Form*. The *Confidential Physician Assessment Form* requests information on any cognitive and physical limitations of the Complainant and their resulting prognosis for return to work. The Corrections' internal investigation report states the following as to what personal health information was in the *Confidential Physician Assessment Form*:

> The Confidential Physician Assessment Form is to be completed by the employee's physician and includes the identification of any restrictions, such as, but not exclusive to lifting, bending, cognitive impairment, limitation due to environment, equipment operation, etc. that would restrict the employee's plan to safely remain at or return to the workplace, how any restrictions would impede [the Complainant's] ability to do the full requirements of the core function of [the Complainant's] position, and the duration and degree of the restrictions. In addition, the physician is asked to identify any supports, plans and goals to address the restrictions, and to confirm if the employee is able to return to work. The employee's diagnosis and conditions are not requested as part of the assessment.

[8] This type of information constitutes the personal health information of the Complainant pursuant to subsection 2(m)(i) of HIPA. Therefore, the first element has been met.

[9] Second, the term trustee is defined by subsection 2(t)(ii) of HIPA as follows:

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

[10] Corrections is a "government institution" and is therefore a "trustee" for purposes of HIPA. As such, the second element is met.

[11] Third, the *Confidential Physician Assessment Form* was collected and retained by Corrections. Therefore, I find that Corrections has custody and control over the personal health information. The third element is met.

[12] As all three elements have been satisfied, I find that HIPA is engaged on these matters.

**2. Was there a privacy breach?**

[13] A privacy breach occurs when personal health information is collected, used and/or disclosed without authority under HIPA. Subsection 24(4) of HIPA provides:

> **24**(4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

[14] Further, subsection 26(3) of HIPA provides restrictions on use of an employee's personal health information as follows:

> **26**(3) Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual's consent.

[15] The Complainant is an employee of Corrections and was on leave from work for medical reasons. The Complainant alleged that they were advised by their physician that Director 1 requested the *Confidential Physician Assessment Form* when they went to Quance East Medical Clinic to pay the associated invoice. The Complainant asserted they did not give consent for anyone other than the Return to Work Specialist (RTWS) to collect or use the personal health information on the assessment.

[16] The Complainant signed a consent form for Corrections titled, *Consent to the Use and Disclosure of Personal Health Information.* The consent form stated:

> …[Physician] will disclose this requested information to:
>
> [RTWS name]
> [address, phone number, fax number]
> Confidential email address: [RTWS email]
>
> [RTWS] will be responsible to ensure that the personal health information collected will be treated as confidential, will be strictly controlled, and will be used and disclosed only to the extent necessary to make such decisions of fitness to work, accommodation arrangements, and employment decisions. I AGREE that my Employer may disclose this information to an authorized third party of disability case management services to assist in making fitness to work decisions and accommodation arrangements. I understand that the personal health information will be kept in a confidential file separate and apart from my personnel file.

[17] In its internal investigation report, Corrections concluded the following:

> The findings conclude there was an unauthorized collection and disclosure of the employee's personal health information. The CTR Director did not read the personal health information contained in the Form so the unauthorized collection and disclosure was kept at a minimum. Once in his possession, the CTR Director took immediate steps to safeguard the employee's personal health information by delivering it to the Director, Reduced Custody Services. After retrieving the Form, the Director, Reduced Custody Services took appropriate measures to ensure the employee's personal health information was safely secured and stored.

[18] At the time it was collected by Director 1, the completed assessment was not in an envelope or concealed in any way. Quance East Medical Clinic did not have consent to disclose it to Director 1 and, according to Corrections, refused to put the information in a sealed envelope when Director 1 requested it to. It appears that part of the responsibility for this breach of privacy also rests with Quance Street Medical Clinic. However, the Complainant has only asked my office to consider the role of Corrections in this matter.

[19] When Director 1 was transporting the Complainant's personal health information, there was another coworker in the vehicle. Director 1 was the passenger and held the completed assessment in his lap. The front page of the assessment package contains personal health information of the Complainant, which would be visible to the coworker given the fact that the assessment was not secured.

[20] On the way back to the office, Director 1 then stopped at the workplace of Director 2 and gave the assessment to them, not the RTWS. Director 2 then scanned the pages, emailed them to the RTWS, and then retained a copy in a locked drawer.

[21] Based on the consent form, it is clear the Complainant consented to their personal health information being provided to the RTWS. However, it was collected by Director 1, shared with Director 2 and was accessible to a co-worker while transporting it.

[22] Corrections acknowledged a breach of privacy occurred when Director 1 picked up the personal health information of the Complainant from Quance East Medical Clinic on February 7, 2019. Corrections does not, however, consider the coworker in the vehicle having access to the personal health information as a privacy breach. Further, it does not

consider the sharing with Director 2 and Director 2's subsequent scanning of each page, as well as then retaining a copy, as breaches of the Complainant's privacy. Corrections also did not advise what happened to the scanned electronic copy of the assessment and whether it has been removed from all electronic storage locations.

[23] The need-to-know principle is the principle that trustees and their staff should only collect, use, or disclose information necessary for purposes authorized by HIPA. The need-to-know principle is enshrined in section 23 of HIPA, which provides:

> **23**(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.

[24] Need-to-know is the principle that personal health information should only be available to those employees in an organization that have a legitimate need-to-know the information for the purpose of delivering their mandated services.

[25] The personal health information, contained within the *Confidential Physician Assessment Form*, was required by Corrections' RTWS in order to assist the employee to return to work effectively. This is who the Complainant consented to receiving their personal health information and the person in the organization with a need-to-know.

[26] Director 1, Director 2 and the co-worker in the vehicle did not have a need-to-know the Complainant's personal health information. Had the medical clinic put the completed assessment in a sealed envelope and sent it directly to the RTWS there would not be an issue. However, by Director 1 picking up the completed assessment, it took custody and control of the personal health information and subsequently the obligations under HIPA were engaged at that moment. More employees than necessary had access to the Complainant's personal health information in this case.

[27] In conclusion, I find that Corrections breached the Complainant's personal health information. This means that at each step in the movement of the Complainant's personal health information, Corrections was not abiding by the consent form signed by the Complainant. It was also not abiding by the need-to-know principle.

**3. Did Corrections respond to this privacy breach appropriately?**

[28] As Corrections has not considered the extent of the breaches, which occurred, I will look at the steps Corrections took to respond to the breach.

[29] My office suggests that trustees undertake the following steps when responding to a privacy breach:

1. contain the breach;
2. notify affected individual(s);
3. investigate the privacy breach; and
4. prevent future privacy breaches.

[30] Below is an analysis of each step.

***1. Contain the breach***

[31] To contain the privacy breach is to ensure that the personal health information is no longer at risk. This may include recovering the record(s), revoking access to personal health information, and/or stopping the unauthorized practice.

[32] Corrections has asked Director 2 to remove the records from their sent email, which occurred when it was scanned and emailed to the RTWS. However, since the original record was still held in the filing cabinet of Director 2, the record is still accessible to Director 2 without a need-to-know.

[33] Corrections has also not advised my office whether any electronic copies of the assessment have been contained.

[34] I find that the breach has not been contained. I recommend that Corrections contain the breach by deleting the Complainant's personal health information from all locations where the paper and electronic assessment is accessible by any persons without a need-to-know.

### *2. Notify the affected individuals*

[35] Notifying the affected individuals of the privacy breach is important so that they can determine how they have been impacted and take steps to protect themselves. A notification should include the following:

- a description of what happened;
- a detailed description of the personal information or personal health information that was involved;
- if known, 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 privacy breaches in the future;
- the contact information of an individual within the organization who can answer questions and provide further information;
- a notice that individuals have a right to complain to the Office of the Information and Privacy Commissioner (IPC);
- the contact information of the IPC, and
- where appropriate, recognition of the impacts of the breach on affected individuals and an apology.

[36] Corrections provided my office with a copy of the notification letter, which they sent to the Complainant. Based on a review of the letter, it contains some of elements although does not include an apology or the steps Corrections will take to prevent similar incidents from happening.

[37] I find the affected individual has been notified, however it is lacking some of the elements my office suggests should be included. I recommend Corrections issue an apology to the Complainant.

### *3. Investigate the privacy breach*

[38] Investigating the privacy breach to identify the root cause is key to understanding what happened and to prevent similar privacy breaches in the future.

[39] Corrections advised that, during its investigation, it interviewed Director 1, Director 2 and the Complainant, but did not provide any evidence that it interviewed the co-worker, the receptionist at Quance East Medical Clinic or the RTWS. A thorough investigation should include interviewing all parties involved in the incident.

[40] I find that Corrections did not complete a thorough investigation.

### *4. Prevent future privacy breaches*

[41] Preventing future breaches means to implement measures to prevent similar breaches from occurring.

[42] Under HIPA, trustees have the responsibility to ensure they have adequate safeguards in place to prevent privacy breaches. Section 16 provides as follows:

> **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.

[43] In order to prevent further breaches, Corrections indicated they will consider:

- All [Program Area] employees complete the online LEARN module entitled "Access and Privacy in the Government of Saskatchewan".

- The [Director 1] should review "A Manager's Guide to Accommodation and Return to Work" and "Section 705: Employment Accommodation" policy available on Taskroom.

[44] Although it is valuable to have all employees take the online *Access and Privacy in the Government of Saskatchewan* training, this training is very high level and does not discuss the type of situation, which occurred.

[45] Corrections also recommends that Director 1 review the Public Service Commission's resource titled, *A Manager's Guide to Accommodation and Return to Work* and it's policy titled, *Return to Work* and *Section 705: Employment Accommodation*. This recommendation is after the incident and Corrections has not advised whether all supervising managers are required to review this material at the time of hire or ongoing. Nevertheless, neither of these resources discuss the type of privacy concerns associated with this incident and their focus is on workplace accommodation and not protection of privacy. In other words, it is too general to assist employees in any tangible way with regards to privacy matters. Therefore, I find that Corrections' recommendations do not provide adequate safeguards to prevent a breach.

[46] Corrections did not abide by section 16 of HIPA, which places a duty to protect personal health information on the trustee with custody and control. I find that the preventative measures suggested by Corrections are not adequate to ensure this type of breach does not occur in the future. I recommend that Corrections develop appropriate procedures to ensure that this type of breach does not occur again.

[47] In conclusion, I find that Corrections did not respond to this breach appropriately.

## III FINDINGS

[48] I find that HIPA is engaged.

[49] I find that the Complainant's privacy was breached.

[50] I find that the breach has not been contained.

[51] I find the Complainant was notified, however, the notification was lacking some of the elements my office suggests should be included.

[52] I find that Corrections did not complete a thorough investigation.

[53] I find that the preventative measures provided by Corrections are not adequate to ensure this type of breach does not occur in the future.

[54] I find that Corrections did not respond to this breach appropriately.

## IV RECOMMENDATIONS

[55] I recommend that Corrections contain the breach by deleting the Complainant's personal health information from all locations where the paper and electronic assessment is accessible by any persons without a need-to-know.

[56] I recommend that Corrections develop appropriate procedures to ensure that this type of breach does not occur again.

[57] I recommend Corrections issue an apology to the Complainant.

Dated at Regina, in the Province of Saskatchewan, this 7th day of January, 2021.

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