Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 140-2019

Saskatchewan Public Safety Agency (formerly Ministry of Environment)

February 7, 2020

Summary: A nurse for Bayshore HealthCare Ltd (Bayshore) conducted fit-for-work assessments on employees within the Wildfire Management Branch of the Saskatchewan Public Safety Agency (SPSA) (which used to be a part of the Ministry of Environment). An employee asserted that the nurse shared the employee's personal health information unnecessarily with the employee's supervisor. Further, the nurse shared inaccurate personal health information. The Commissioner made several findings, including that there was no authority under *The Health Information Protection Act* (HIPA) for the sharing of the employee's personal health information with the employee's supervisor. Further, the Commissioner found that SPSA (formerly the Ministry) has not taken reasonable steps to ensure the accuracy and completeness of the personal health information in this case. The Commissioner made several recommendations including contacting the employee to inform them of their right to access and their right to request amendments to their personal health information under HIPA. The Commissioner also recommended that the SPSA conduct an inspection of Bayshore.

I BACKGROUND

[1] On May 11, 2018, the Ministry of Environment (the Ministry) proactively reported a privacy breach that affected 37 individuals, to my office. My office made six recommendations. The Ministry agreed to comply with the six recommendations. Therefore, my office considered the matter informally resolved without issuing a report. I will refer to this previous investigation by my office throughout this Investigation Report.

[2] One of my office's recommendations in the previous investigation was for the Ministry to notify the 37 affected individuals of their right to complain to my office. After receiving a notice from the Ministry, one of the affected individuals submitted a complaint to my office. This person will be referred to as the Complainant. The background for the complaint is described below.

[3] The Ministry has had a contract with Bayshore HealthCare Ltd (Bayshore) for the past 11 years to conduct fit-for-work assessments on its employees within the Wildfire Management Branch. The process for conducting fit-for-work assessments is as follows:

1. The employee fills out a Physical Activity Readiness Questionnaire (PARQ) form.
2. Depending on how the employee fills out the PARQ form, a Bayshore nurse may follow up with the employee to conduct a fit-for-work assessment.
    a. If the Bayshore nurse does indeed conduct an assessment, he/she will fill out a fit/not-fit-to-work form.
        i. The fit/not-fit-to-work form provides a "yes" or "no" as to whether or not the employee is fit to work. It should **not** contain any other personal health information about the employee, such as notes/comments by the nurse.
3. The Bayshore nurse sends the completed fit/not-fit-to-work form to the employee's supervisor at the Ministry.
4. Bayshore retains the PARQ form and any notes/comments by the nurse.

[4] As noted in the above steps, the Bayshore nurse is *not* to send personal health information about the employee to the employee's supervisor. The Bayshore nurse is supposed to only send a form that indicates whether the employee is fit-to-work or not. However, a Bayshore nurse sent 37 fit/not-fit-to-work forms containing Ministry employees' personal health information to the employees' supervisors in 2017 and 2018, before the Ministry became aware that it was receiving more information than it should have.

[5] As described earlier, the Complainant submitted a complaint to my office. The Complainant was familiar with this assessment process as they had worked for the Ministry for several years and had gone through the process every year. As they had done in the past, the Complainant had filled out the PARQ form. Then, they received a call from a Bayshore nurse requesting information about their medical condition. The Complainant, who expected that any information they provided to the Bayshore nurse would be kept confidential, provided information about their medical condition.

[6] The Bayshore nurse filled out the fit/not-fit-to-work form and then emailed the form to the Occupational Health and Safety (OH&S) Coordinator at the Ministry, who is the Complainant's supervisor.

[7] The Ministry's OH&S Coordinator then forwarded the form to the Complainant. The Complainant noticed that not only did the form contain more information than it should, it contained incorrect information about their medical condition. The Complainant reported their concern to the Ministry's OH&S Coordinator.

[8] In an email dated March 28, 2018, the Ministry's OH&S Coordinator contacted Bayshore about the privacy breach.

[9] On April 20, 2018, Bayshore sent a letter to the Complainant. The letter explained the findings of Bayshore's investigation into the sharing of the Complainant's personal health information with the Ministry's OH&S Coordinator, and what Bayshore had done to respond to this privacy breach. The letter included an apology and also the contact information of a director at Bayshore that the Complainant can contact if they had any questions or concerns. While the letter addressed the inappropriate sharing of personal health information with the Ministry, the letter did not respond to the Complainant's concerns over the inaccuracy of the personal health information that was recorded by the Bayshore nurse.

[10] On May 7, 2018, the Complainant contacted their manager by email to express how they were still concerned with the process. The Complainant raised not only the issue of their personal health information being shared inappropriately, but also how their personal health information was incorrect. The Complainant expressed concern about the Bayshore nurse using incorrect information to determine whether the affected individual is fit to work or not. The Complainant called into question Bayshore's credibility.

[11] The Complainant's manager responded indicating the Ministry is working with Bayshore to respond to the privacy breach. The Manager also encouraged the affected individual to contact Bayshore to discuss their concerns.

[12] Then, as indicated earlier, the Ministry proactively reported the privacy breach that affected 37 individuals to my office on May 11, 2018. It should be noted that at the time the Ministry proactively reported the breach to my office, it did not report any specific details about the Complainant's case to my office. My office reviewed the Ministry's safeguards for this process of assessing employees on whether they are fit-to-work or not and made six recommendations, including notifying all 37 affected individuals that they have a right to complain to my office. The Ministry agreed to comply with my office's recommendations. Therefore, my office closed its file on April 15, 2019.

[13] In a letter dated April 22, 2019, as a part of the Ministry's compliance with my office's recommendations, the Ministry notified the Complainant that they have a right to complain to my office. On May 6, 2019 and May 10, 2019, the Complainant contacted my office by telephone and by email.

[14] On May 27, 2019, my office notified both the Complainant and the Ministry that my office would be undertaking an investigation.

[15] In November of 2019, the Wildfire Management Branch was transferred from the Ministry to the Saskatchewan Public Safety Agency (SPSA). This Report will reference the Ministry since the privacy breach occurred when the Ministry was the trustee of the personal health information at issue. However, since the SPSA is now the trustee responsible for fit-for-work assessments, the recommendations will be for SPSA.

II DISCUSSION OF THE ISSUES

1. Is *The Health Information Protection Act* (HIPA) engaged and do I have jurisdiction to investigate this matter?

[16] HIPA is engaged when there are three elements present: 1) a trustee, 2) personal health information, and 3) the trustee has custody or control over the personal health information. Subsection 2(t) of HIPA defines "trustee" 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;

[17] The Ministry is a "government institution" as defined by subsection 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP). Furthermore, the SPSA is a "government institution" as defined by subsection 2(1)(d)(ii) of FOIP. Therefore, both the Ministry and SPSA would also qualify as trustees under HIPA.

[18] In this case, Bayshore (a contractor of the Ministry) is collecting information about employees' health for the purpose of the assessments. Subsection 2(m) of HIPA 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;

[19] Finally, there is a contract between the Ministry and Bayshore that provides that the Ministry has control over the personal health information.

[20] Based on the above, I find that HIPA is engaged.

[21] Subsection 52(d) of HIPA provides as follows:

> **52** The commissioner may:
> ...

> (d) from time to time, carry out investigations with respect to personal health information in the custody or control of trustees to ensure compliance with this Act;

[22] I find that I have jurisdiction and authority to investigate this matter.

2. Did the Ministry take reasonable steps to ensure the personal health information collected was accurate and complete?

[23] Bayshore collects personal health information on behalf of the Ministry. In this case, the Complainant alleged that the Bayshore nurse collected and recorded incorrect personal health information about them. As described in the background section of this Report, the Complainant raised this concern with the Ministry in their email dated May 7, 2018. The Ministry responded by encouraging the Complainant to contact Bayshore.

[24] One of the duties set out in Part III of HIPA is for trustees to take reasonable steps to ensure they are collecting complete and accurate personal health information. Collecting accurate and complete information is important as such information is used to assess whether employees are fit-to-work or not. Section 19 of HIPA provides as follows:

> **19** In collecting personal health information, a trustee must take reasonable steps to ensure that the information is accurate and complete.

[25] To "take reasonable steps" means that the trustee will be thorough in identifying practicable means to ensure that the personal health information is accurate and complete. Having a procedure in place to ensure that individuals can request access to their personal health information as well as another procedure in place to ensure that individuals can request an amendment to their personal health information are methods that a trustee can undertake to ensure personal health information is accurate and complete.

[26] As mentioned in the background section, the Ministry has had a contract with Bayshore for the past 11 years. Furthermore, the Complainant has completed this assessment process every year for several years. It is difficult to know the extent, if any, of the inaccuracy of the Complainant's personal health information, because the Ministry's response to the

Complainant's email dated May 7, 2018, was for the Complainant to contact Bayshore about their concern. If the personal health information is indeed inaccurate, it is possible the inaccuracy has existed and persisted over several years and not simply contained to a single year. However, the Complainant's allegation that the Bayshore nurse collected and recorded inaccurate personal health information has not been investigated by the Ministry.

[27] I find that the Ministry has not taken reasonable steps to ensure the accuracy and completeness of the personal health information in this case.

[28] Recently, the Ministry amended its agreement with Bayshore so that a process is in place to facilitate formal access to information requests under HIPA. I commend the Ministry and Bayshore for making such an amendment. In terms of a procedure for individuals requesting amendments to their personal health information pursuant to section 40 of HIPA, the Ministry directs them to contact Bayshore. Its internal investigation report provides as follows:

> No amendments are made to the PHI [personal health information] collected by the ministry and employees are directed to contact Bayshore with requests for amendments to their PHI. Amendments are to be made by the same nursing staff member assigned to assess the employee to maintain confidentiality.

[29] First, I recommend that the contract be amended so that the contract is between the SPSA and Bayshore.

[30] Second, since it is the SPSA that is responsible for ensuring compliance with HIPA, I recommend that the SPSA take the lead in responding to requests for amendments to personal health information pursuant to section 40 of HIPA, instead of requiring Bayshore to respond to such requests. SPSA and Bayshore should work together to respond to such requests for amendments, but only those who have a need-to-know should be a part of responding to the requests for amendments in order to maintain confidentiality.

[31] Third, I recommend that SPSA contact the Complainant to notify them of their right of access to their personal health information and their right to request amendment to the

personal health information. If the Complainant wishes to proceed, the Complainant should submit a formal access to information request for their personal health information and they should be provided access to their personal health information that is in the custody of Bayshore (subject to limited and specific exemptions set out in section 38 of HIPA). Once the Complainant receives their personal health information, the Complainant should be able to determine if they wish to request amendment to their personal health information. Requiring the Complainant to submit formal requests pursuant to sections 12, 32, and 40 of HIPA is to ensure they maintain their right to appeal to my office pursuant to section 42 of HIPA.

[32] Fourth, I recommend that the SPSA determine a method of notifying Wildfire Management Branch employees (past and present) who have been through the assessment process of their right of access to personal health information pursuant to sections 12 and 32 of HIPA, and their right to request amendment pursuant to section 40. If errors have been made in the past, then hopefully individuals will have an opportunity to request amendments.

[33] Fifth, I recommend that the SPSA make it a practice to let employees know of their rights pursuant to sections 12, 32, and 40 of HIPA at the same time that employees are asked to fill out the PARQ form.

[34] Finally, as noted above, the Ministry has not conducted any inspection of Bayshore. I recommend that the SPSA conduct an inspection of Bayshore to ensure that Bayshore is complying with the contract. The inspection should include ensuring Bayshore is completing the work as outlined in Schedule A of the contract (i.e. not recording personal health information on fit/not-fit-to-work forms) as well as maintaining records pursuant to the retention and destruction schedule set out in the contract.

3. Was there authority in HIPA for the sharing of the Complainant's personal health information?

[35] Subsection 2(u) of HIPA defines "use" as follows:

> **2** In this Act:
>
> ...
> (u) "use" includes reference to or manipulation of personal health information by the trustee that has custody or control of the information, but does not include disclosure to another person or trustee.

[36] Since Bayshore was a contractor for the Ministry, Bayshore created and stored records that were under the control of the Ministry. Therefore, the sharing of personal health information between Bayshore and the Ministry qualified as a "use" of personal health information.

[37] Subsections 23(1) and 23(2) of HIPA provides that personal health information should only be used on a need-to-know basis. They provide as follows:

> **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.

[38] As set out in the background section, the Ministry had a procedure for conducting fit-for-work assessments so that only those with a need-to-know personal health information has access to such information. I find that this procedure was in accordance with subsection 23(2) of HIPA.

[39] In this case, the Bayshore nurse unnecessarily recorded the Complainant's personal health information on the fit/not-fit-to-work form and then sent the form to the Complainant's supervisor. This recording and sharing of the Complainant's personal health information was not in accordance with the process for conducting fit-for-work assessments. The Complainant's supervisor only needed to know if the Complainant was fit-to-work and not other personal health information. Therefore, subsection 23(1) of HIPA did not authorize the sharing of the personal health information by the Bayshore nurse with the Ministry. I therefore find a privacy breach occurred.

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

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

- Contain the breach,
- Notify affected individual(s),
- Investigate the privacy breach,
- Prevent future privacy breaches, and
- Write an investigation report.

[41] Below is an analysis of each step.

Contain the breach

[42] Upon learning that a privacy breach has occurred, trustees should immediately take steps to contain the breach. To contain a 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 the personal health information, and/or stopping the unauthorized practice.

[43] Soon after the Ministry discovered that Bayshore was sharing more personal health information than it should, the Ministry contacted Bayshore. Bayshore began its own investigation into the matter.

[44] Further, the Ministry's Privacy Officer issued the directive to permanently delete the emails and destroy paper copies placed on employees' personnel files. Further, the Ministry's Privacy Officer did the following:

- Spoke directly to each of the eleven supervisors potentially affected to inform them of what has occurred and outlined the expectation that they are to destroy the records,
- Contacted Bayshore so that Bayshore can begin notifying not only the Complainant in this case, but also the 36 other affected individuals, and
- Contacted the Ministry's Crown counsel to advise of what has occurred.

[45] On April 9, 2018, the Ministry confirmed that it had destroyed both electronic and paper copies of personal health information it received from Bayshore. I find that the Ministry has contained the breach.

[46] I recommend that the SPSA keep evidence of the privacy breach until at least its own investigation into the matter is complete. If my office is involved, then I recommend that the SPSA maintain the evidence until my office's investigation is complete.

Notify affected individuals

[47] It is important that trustees notify affected individuals when a privacy breach has occurred. Not only do the affected individuals have a right to know, they need to know, in order to protect themselves from any potential harm that may result from the privacy breach. Unless there is a compelling reason not to, trustees should always notify affected individuals. An effective notification should include:

- A description of what happened;
- A detailed description of the personal health 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 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 and its contact information; and
- Recognition of the impacts of the breach on affected individuals and an apology.

[48] As mentioned in the background, Bayshore wrote a letter dated April 20, 2018, to the Complainant to notify them of the privacy breach and to apologize. Furthermore, Bayshore sent a letter to the other affected individuals to notify them of the privacy breach.

[49] In the previous investigation, my office noted that even though the affected individuals were notified of the privacy breach, they were not made aware of their right to complain to my office. Therefore, my office recommended that the Ministry notify the affected

individuals of their right to complain to my office. The Ministry complied with that recommendation. As a result, the Complainant submitted the complaint to my office.

[50] I find that the Ministry has notified the Complainant and the other affected individuals of the privacy breach.

Investigate the breach

[51] Trustees should investigate privacy breaches with the goal of identifying the root causes. Understanding the root causes enables trustees to develop and implement plans to prevent similar privacy breaches in the future.

[52] During my office's previous investigation, the Ministry had indicated that one of the root causes was the inadequate training of the Bayshore nurse. Another root cause was that that the Ministry failed to detect the privacy breach when it began to receive fit/not-fit-to-work forms containing personal health information in 2017. It discovered the privacy breach after receiving 37 fit/not-fit-to-work forms. Finally, during the previous investigation, my office noted that the Ministry's agreement with Bayshore did not explicitly state that Bayshore is not to share personal health information with the Ministry. Therefore, my office identified that the ambiguity in the contract could have contributed to the privacy breach.

[53] I find that the Ministry has investigated the unauthorized sharing of personal health information.

[54] As noted at paragraphs [26] and [27], I find that the Ministry has not investigated the alleged inaccurate collection and recording of personal health information by the Bayshore nurse.

Preventing similar privacy breaches

[55] Once a trustee has identified the root cause of a privacy breach, then it should develop and implement a plan to prevent a similar privacy breach from occurring.

[56] To address the above root causes, the Ministry did the following:

- Removed the comments section on the fit/not-fit-to-work form so there is no space or prompts for the nurse to record personal health information.
- Developed a privacy training course which teaches Ministry employees and managers of what a privacy breach is and to contact the Ministry's Privacy Officer if they suspect a privacy breach has occurred.
- Committed itself to sending out reminders to Ministry supervisors and to Bayshore (or any contracted health care provider) of the procedures and emphasizing the need to identify any discrepancies on the forms in a timely manner.
- Appended two of the Ministry's internal procedures, TAS611.1 and TAS611.2, to the contract with Bayshore. These two internal procedures set out the procedures that are to be followed, including explicitly stating that personal health information should not be recorded on the fit/not-fit-to-work form.

[57] I find that the Ministry has taken steps to minimize the likelihood of the unauthorized sharing of personal health information.

[58] In addition, in its letter dated April 20, 2018 to the Complainant, Bayshore has indicated that it has "modified our orientation/reference materials and processes to ensure this will never happen again". I recommend that SPSA review Bayshore's "orientation/reference materials" to verify they are consistent with SPSA's processes as well as the contract. Further, pursuant to Schedule A of the contract, Bayshore is to meet with the Ministry's (or SPSA's) OH&S Coordinator twice per term of the contract. I recommend that during these meetings, SPSA set out the expectations of how Bayshore is to manage personal health information to maintain privacy and confidentiality.

Write an investigation report

[59] Documenting a trustee organization's investigation into a privacy breach is a method to ensure that the trustee organization follows through with plans to prevent similar breaches in the future.

[60] The Ministry has provided my office with an investigation report. I find that the Ministry has fulfilled this step in responding to a privacy breach.

III FINDINGS

[61] I find that HIPA is engaged.

[62] I find that I have jurisdiction and authority to investigate this matter.

[63] I find that the Ministry has not taken reasonable steps to ensure the accuracy and completeness of the personal health information in this case.

[64] I find that there was no authority in HIPA for the sharing of the personal health information.

[65] I find that the Ministry has contained the breach.

[66] I find that the Ministry has notified the Complainant and the other affected individuals of the privacy breach.

[67] I find that the Ministry has investigated the unauthorized sharing of personal health information.

[68] I find that the Ministry has not investigated the alleged inaccurate collection and recording of personal health information by the Bayshore nurse.

[69] I find that the Ministry has taken steps to minimize the likelihood of the unauthorized sharing of personal health information.

IV RECOMMENDATIONS

[70] I recommend that the SPSA contact the Complainant to notify them of their right of access to their personal health information and their right to request amendment to the personal health information as described at paragraph [31].

[71] I recommend that the SPSA determine a method of notifying Wildfire Management Branch (past and present) who have been through the assessment process of their right of access to personal health information pursuant to sections 12 and 32 of HIPA, and their right to request amendment pursuant to section 40 of HIPA as described at paragraph [32].

[72] I recommend that the SPSA make it a practice to let employees know of their rights pursuant to sections 12, 32, and 40 of HIPA at the same time that employees are asked to fill out the PARQ form.

[73] I recommend that the SPSA conduct an inspection of Bayshore to ensure that Bayshore is complying with the contract as described at paragraph [34].

[74] I recommend that the SPSA keep evidence of the privacy breach until at least its own investigation into the matter is complete. If my office is involved, then I recommend that the SPSA maintain the evidence until my office's investigation is complete.

[75] I recommend that the SPSA review Bayshore's "orientation/reference materials" to verify they are consistent with the SPSA's processes as well as the contract.

[76] I recommend that during meetings with Bayshore, the SPSA set out the expectations of how Bayshore is to manage personal health information to maintain privacy and confidentiality as described at paragraph [58].

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

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