Office of the
Saskatchewan Information
and Privacy Commissioner

# INVESTIGATION REPORT 042-2017

## Ministry of Health

**April 7, 2017**

**Summary:** In a previous investigation, the Commissioner found that a doctor had inappropriately accessed personal health information in the Pharmaceutical Information Program (PIP). The Ministry of Health (Health) is the trustee, as defined by *The Health Information Protection Act* (HIPA), for PIP. Therefore, the Commissioner investigated Health's role in responding to the doctor's inappropriate accessing of personal health information in PIP. He made a number of recommendations, including notifying all affected individuals of the doctor's inappropriate access within 30 days issuing this Investigation Report and that Health audit the doctor and his employees' use of PIP.

## I BACKGROUND

[1] In Investigation Report 282-2016, my office found that Dr. Haidash of Eastside Medical Clinic had inappropriately accessed personal health information on the Pharmaceutical Information Program (PIP). That Investigation Report also noted that Dr. Haidash was charged by the Council of the College of Physicians and Surgeons of Saskatchewan (CPSS) of improperly accessing the personal health information of a number of individuals through PIP without a legitimate need-to-know in or about January 23 to 25 of 2009. Dr. Haidash admitted he was guilty of the charge according to an admission he signed on November 4, 2016.

[2] The Ministry of Health (Health) is the trustee, as defined by subsection 2(t)(i) of *The Health Information Protection Act* (HIPA), as it is responsible for PIP. Therefore, in an email dated March 9, 2017, my office notified Health that it was initiating an

investigation into Health's role in responding to Dr. Haidash's inappropriate access of personal health information.

## II DISCUSSION OF THE ISSUES

[3] Health is a trustee pursuant to subsection 2(t) of HIPA.

### 1. Did Health respond appropriately to the privacy breach?

[4] My office has already found there was a privacy breach, as detailed in Investigation Report 282-2016. Where there is a privacy breach, my office's focus is determining whether the trustee has appropriately handled the privacy breach. My office recommends five best practice steps to be taken when responding to a privacy breach. These five steps are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Plan for prevention,
5. Prepare an Investigation Report.

[5] I will use these five steps to assess Health's response to the privacy breach.

#### Contain the Breach

[6] Containing the breach means taking action so that personal health information is no longer at risk. This may involve the following:

- stopping the unauthorized practice,
- recovering the records,
- shutting down the system that was breached,
- revoking access to personal health information,
- correcting weaknesses in physical security.

[7] In this case, suspending or revoking Dr. Haidash's access to PIP would have been effective in containing the breach. However, there is no indication that Dr. Haidash's access to PIP had been suspended or revoked.

[8] According to its submission, Health received a complaint from an affected individual on July 28, 2014. The affected individual felt that Dr. Haidash's access to her PIP profile on January 24, 2009 at 2:09 p.m. was inappropriate.

[9] Health investigated the complaint and determined the following:

- That Dr. Haidash had not submitted any billing to Health's Medical Service Branch related to the affected individual,
- That no prescription or dispensation had occurred related to the affected individual.

[10] In a letter dated August 18, 2014, Health requested that Dr. Haidash respond to the allegation of inappropriately accessing the affected individual's PIP profile. Further, in a letter dated September 3, 2014, Health indicated that it had determined, "in a period of less than 25 minutes, [Dr. Haidash] viewed and potentially printed the prescription information of 18 people." Health indicated to Dr. Haidash that it was expanding its investigation to include the viewing of 18 people's personal health information in less than 25 minutes. Health requested that Dr. Haidash respond to Health's finding.

[11] According to Health's submission, Dr. Haidash's solicitor responded to Health on September 11, 2014. The response was as follows:

- Dr. Haidash does not have a specific recollection of accessing particular profiles in question on January 24, 2009;
- Around this time in 2009, Dr. Haidash was teaching his wife to assist in various aspects of his medical practice, including PIP,
- January 24, 2009 was a Saturday so Dr. Haidash's clinic would not have been open so there would not have been any medical reason to access the profiles,
- Dr. Haidash has never met the affected individual,
- To the best of his knowledge, there is no connection between the additional names of individuals' whose PIP profiles were accessed and the affected individual.

[12] As Health was conducting its investigation, the CPSS initiated its own investigation. It appears that Health suspended its investigation into the breach until it was notified by my office in March 2017 that my office was undertaking its own investigation. Through this notification, Health learned the CPSS issued its final decision.

[13] From the time Health received the complaint from the affected individual on July 28, 2014 to March 2017, it does not appear that Dr. Haidash's access to PIP was suspended or revoked. Certainly, receiving a complaint that alleges of inappropriate access is not, in and of itself, enough to suspend or revoke access to PIP. However, Health should have at least suspended Dr. Haidash's access to PIP in August 2014, as soon as it had determined that 1) Dr. Haidash had accessed the affected individual's PIP profile on January 24, 2009 at 2:09 p.m., 2) Dr. Haidash had not submitted any billing for medical services related to the Complainant and, 3) no prescription or dispensation occurred related to the affected individual. There was enough evidence to support the affected individual's allegation. At that point, Health should have suspended Dr. Haidash's access to PIP until Dr. Haidash responded to its letters dated August 18, 2014 and September 3, 2014 and Health was satisfied that Dr. Haidash would not (or was not) accessing personal health information inappropriately on PIP. I find that Health did not appropriately contain the breach.

**Notify affected individuals and/or appropriate organizations**

[14] In Investigation Report 282-2016, my office determined there may be 17 additional individuals, who may have had their personal health information accessed inappropriately by Dr. Haidash on January 24, 2009.

[15] Based on its letter dated September 3, 2014 to Dr. Haidash, Health was already aware that there were additional affected individuals. In its submission, Health has committed to notifying all the affected individuals by letter and it will include a sincere apology, a description of the privacy breach and subsequent investigation, the circumstances and the personal health information involved, strategies it has in place or is planned to mitigate the harm and prevent future breaches, and Health's contact information and my office's contact information should any of the individuals wish to follow-up on this breach. While I am pleased that Health will be notifying the other affected individuals, I find that Health should have notified these individuals soon after it discovered that there may have been inappropriate access into their personal health information on PIP. That would enable

these individuals to take action to mitigate any harm coming from the inappropriate access, including masking their personal health information in PIP.

[16] If it has not done so already, I recommend that Health notify all the affected individuals within 30 days of my office issuing its Final Investigation Report.

**Investigate the breach**

[17] The goal of investigating a breach is to find out what happened and to hopefully uncover the root cause of the breach.

[18] As described earlier, Health had received a complaint from the affected individual on July 28, 2014. Its investigation included determining that Dr. Haidash had not submitted any billing for medical services related to the affected individual and that there were no prescriptions or dispensation that occurred related to the affected individual. Health was also able to establish there may have been additional individuals affected by inappropriate access into their PIP profiles by Dr. Haidash.

[19] In its submission to my office, Health indicated it will work with its Information Management Service Provider (IMSP) for PIP, eHealth Saskatchewan (eHealth), and CPSS to ensure that members of CPSS are aware of their responsibilities as users of PIP and that training materials are readily available on the eHealth website. It said it will also work with eHealth to review PIP system auditing and to discuss and determine whether future targeted audits should be implemented for Dr. Haidash. It said it will also review its Privacy Breach Management Guidelines and improve its communication between Health and other bodies and trustees. Based on its commitments, Health appears to acknowledge that factors contributed to the privacy breach was the lack of awareness/training and auditing.

[20] While I find that Health's initial efforts in its investigation and Health's commitments going forward are appropriate, I need to address that it appears Health's investigation was suspended while CPSS initiated its investigation into the breach. As a part of its review of

its Privacy Breach Management Guidelines, I recommend that Health continue its investigation into a breach regardless of whether or not CPSS or any other body are conducting an investigation. This is important so that Health can identify and repair any inadequacies in its safeguards in a timely fashion.

**Plan for prevention**

[21] As noted in paragraphs [15] and [19], Health will:

1. Notify the other affected individuals,
2. Work with eHealth and CPSS to ensure members of CPSS are aware of their responsibilities and the training materials available on the eHealth website,
3. Work with eHealth regarding PIP system auditing and to determine if future targeted audits should be implemented for Dr. Haidash, and
4. Review its Privacy Breach Management Guidelines and improve its communication between Health, other bodies, and trustees.

[22] As noted earlier, I find that Health's commitments going forward are appropriate. In addition, I recommend that Health commence a thorough audit of Dr. Haidash and his employees at his medical clinic to ensure that they are using PIP in accordance with HIPA and Health's Joint Service & Access Policy within 60 days of this Final Investigation Report being issued. This should include ensuring personal health information is being accessed only on a need-to-know basis. Based on that audit, if Health determines that Dr. Haidash and/or his employees are not in compliance, then I recommend that Health suspend Dr. Haidash and his employees' access to PIP until they are in compliance. If Dr. Haidash and his employees are already in compliance with the Joint Service & Access Policy, or once they become compliant, then I recommend that Health conduct regular annual audits on Dr. Haidash and his employees for at least three years.

**Prepare an Investigation Report**

[23] Health provided my office with its submission, which appears to be also its investigation report into this breach. It includes a background and chronology of events, summary of actions it has undertaken to investigate, its findings, and actions and its plans to prevent a

similar breach in the future. Its investigation report includes documents related to its investigation.

[24] I find that Health's investigation report to be comprehensive. It deals with documenting the breach, its investigation, its findings, and its plans to prevent a similar breach in the future.

## IV FINDINGS

[25] I find that Health did not appropriately contain the breach.

[26] I find that Health has not notified affected individuals.

[27] I find that Health's initial efforts in its investigation into the privacy breach were appropriate.

[28] I find that Health suspending the investigation prevented it from identifying and repairing inadequacies in its safeguards in a timely fashion.

[29] I find that Health's commitments described in paragraph [21] to prevent a similar breach in the future are appropriate.

[30] I find that Health's investigation report to be comprehensive. It deals with documenting the breach, its investigation, its findings, and its plans to prevent a similar breach in the future.

## V RECOMMENDATIONS

[31] If it has not done so already, I recommend that Health notify all the affected individuals within 30 days of my office issuing this Report.

[32] I recommend that Health commence a thorough audit of Dr. Haidash and his employees at his medical clinic to ensure that they are using PIP in accordance with HIPA and

Health's Joint Service & Access Policy within 60 days of my office issuing this Report. This should include ensuring personal health information is being accessed only on a need-to-know basis.

[33] I recommend that Health suspend Dr. Haidash and/or his employees' access to PIP if the audit reveals they are not in compliance with HIPA and Health's Joint Service & Access Policy.

[34] If/when Dr. Haidash is in compliance with HIPA and Health's Joint Service & Access Policy, I recommend that Health conduct regular annual audits on Dr. Haidash and his employees for at least three years.

Dated at Regina, in the Province of Saskatchewan, this 7th day of April, 2017.

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