Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 282-2016

Eastside Medical Clinic (Dr. Serhii Haidash)

March 28, 2017

Summary: The Complainant requested and received a copy of a Pharmaceutical Information Program (PIP) audit report and discovered that Dr. Serhii Haidash of Eastside Medical Clinic had accessed her patient profile on PIP. The Office of the Information and Privacy Commissioner (IPC) found that Dr. Haidash's access of personal health information on PIP on January 24, 2009 was not in compliance with *The Health Information Protection Act* (HIPA).

I BACKGROUND

[1] The Complainant requested a Pharmaceutical Information Program (PIP) audit report from the Ministry of Health (Health). Since eHealth Saskatchewan (eHealth) is Health's Information Management Service Provider for PIP, eHealth provided the Complainant with a copy of her PIP audit report.

[2] A PIP audit report lists the health care providers who have accessed an individual's patient profile in PIP. When the Complainant received her PIP audit report, she noticed that Dr. Serhii Haidash of Eastside Medical Clinic had accessed her patient profile in PIP on January 24, 2009. She had never been a patient of Dr. Haidash.

[3] The Complainant complained to the College of Physicians and Surgeons. According to charges by the Council of the College of Physicians and Surgeons, Dr. Haidash had improperly accessed 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 that was signed on November 4, 2016.

[4] On November 29, 2016, the Complainant requested that my office investigate this matter.

[5] On December 8, 2016, my office notified Eastside Medical Clinic and the Complainant that it would be undertaking an investigation.

II DISCUSSION OF THE ISSUES

1. Is *The Health Information Protection Act* (HIPA) engaged in this matter?

[6] In order for HIPA to be engaged, three elements must be present: 1) a trustee, 2) personal health information, and 3) the trustee has custody or control over the personal health information.

[7] First, Dr. Haidash of the Eastside Medical Clinic qualifies as a trustee pursuant to subsection 2(t)(xii) of HIPA.

[8] Second, a patient profile within PIP contains information such as the medication information and/or allergy or intolerance information about an individual. 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;

[9] Based on the above, there is personal health information involved in this matter.

[10] Third, by having accessed personal health information on PIP, Dr. Haidash had custody of personal health information. As noted in previous Investigation Reports by my office, including Investigation Report H-2010-001, Health is the trustee of PIP. When a trustee enters into the PIP system and views personal health information, Health is disclosing the

personal health information and the trustee is collecting the personal health information. This collection means that the trustee, Dr. Haidash, collected the personal health information.

[11] Based on the above, all three elements are present. Therefore, I find that HIPA is engaged.

2. Was Dr. Haidash's access to the Complainant's PIP profile in accordance with section 26 of HIPA?

[12] A trustee must only use personal health information in accordance with section 26 of HIPA. Section 26 of HIPA provides:

> 26(1) A trustee shall not use personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section.
>
> (2) A trustee may use personal health information:
>
> (a) for a purpose for which the information may be disclosed by the trustee pursuant to section 27, 28 or 29;
> (b) for the purposes of de-identifying the personal health information;
> (c) for a purpose that will primarily benefit the subject individual; or
> (d) for a prescribed purpose.
>
> (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.

[13] In a letter dated December 23, 2016 to my office, Dr. Haidash's solicitor asserted that since the access was almost eight years ago, Dr. Haidash does not have a specific recollection of accessing the Complainant's profile. However, Dr. Haidash believes he was using the personal health information to train his wife to assist with various aspects of his medical practice.

[14] I find that section 26 does not authorize the use of personal health information for the purpose of training.

3. Was Dr. Haidash's access to the Complainant's PIP profile in accordance with section 23 of HIPA?

[15] The need-to-know principle means that personal health information should only be available to those employees in a trustee organization that have a legitimate need-to-know the information for the purpose of a program or activity of the trustee organization. An example of a legitimate need-to-know in the context of a medical clinic is when a patient presents him or herself to a doctor and the doctor needs to access the patient's personal health information in order to provide care. The need-to-know principle is encoded into 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.
> (3) Repealed.
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

[16] According to Dr. Haidash's submission, Dr. Haidash has never met the Complainant nor has she ever been a patient of his. I find that since the Complainant has never been a patient at Eastside Medical Clinic, then Dr. Haidash would not have had a need-to-know the Complainant's personal health information. Therefore, I find that Dr. Haidash's access to the Complainant's personal health information on PIP on January 23, 2009 was not in compliance with section 23 of HIPA. This finding is also supported by the charges by the Council of the College of Physicians and Surgeons and the admission signed by Dr. Haidash, as described in the background section.

[17] Furthermore, subsection 23(2) requires that trustees have policies and procedures in place 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 HIPA. Dr.

Haidash enabled his wife to use his PIP account to search personal health information suggests that he did not have adequate policies or procedures in place to restrict her access to personal health information in PIP. If Dr. Haidash's wife was an employee of the Eastside Medical Clinic, and if she legitimately needed access to PIP to complete her job duties, then he should have registered her with her own user account on PIP.

[18] In the course of this investigation, my office requested that Dr. Haidash provide my office with copies of policies and/or procedures he has in place regarding the accessing of personal health information on electronic systems such as PIP. On March 27, 2017, my office was informed that Dr. Haidash is developing such policies. My office received a draft of a policy booklet entitled "Privacy and Security Policy and Procedures Manual" dated March 2017. Dr. Haidash has submitted this draft policy booklet to his solicitor for review to ensure it is complete and compliant. His solicitor also said he would be happy to consider any comments my office would have on the draft policy booklet. Therefore, my office will review and provide comment for Dr. Haidash's consideration prior the finalization of the policy booklet.

[19] While I find that Dr. Haidash is not in compliance with subsection 23(2) of HIPA because he has not had any sort of policy or procedures in place prior to this investigation, he is taking the appropriate steps to become compliant with subsection 23(2) of HIPA.

4. Was Dr. Haidash's access of the Complainant's PIP profile in accordance with section 16 of HIPA?

[20] Section 16 of HIPA requires trustees establish policies and procedures to maintain administrative, technical and physical safeguards that will protect the personal health information. 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.

[21] In the submission, Dr. Haidash's solicitor said that at the time that Dr. Haidash accessed the Complainant's personal health information, there were very few guidelines or training resources available and that Dr. Haidash was left to use his own discretion on how to train staff.

[22] There very well could have been few guidelines or training resources available in January 2009. However, this does not negate Dr. Haidash's duties and responsibilities under HIPA. The integrity, accuracy and confidentiality of personal health information is threatened or compromised when personal health information is accessed without a need-to-know.

[23] I find that Dr. Haidash was not in compliance with section 16 of HIPA at the time the Complainant's personal health information was accessed.

[24] As noted earlier, Dr. Haidash is developing a policy booklet entitled "Privacy and Security Policy and Procedures Manual" dated March 2017. While I find that Dr. Haidash is still not in compliance with section 16 of HIPA because he does not have policies and/or procedures in place, he is taking the appropriate steps to become compliant with section 16 of HIPA.

5. Has this privacy breach been dealt with adequately?

[25] Dr. Haidash's solicitor describes how the College of Physicians and Surgeons have conducted an investigation into this matter, have given Dr. Haidash a reprimand, ordered Dr. Haidash to pay the costs of the investigation, and directed Dr. Haidash to take "certain educational resources on privacy". Further, he says that Dr. Haidash has apologized to the Complainant "for any misunderstanding or concern on her part." Based on this, he asserts that "this matter has been fully aired, investigated and dealt with, and that no further action is necessary."

[26] I disagree. First, even though the College of Physicians and Surgeons has conducted an investigation, my office is independent of the College of Physicians and Surgeons. It has the ability to conduct its own investigation under HIPA and make its own findings and recommendations. Second, based on a PIP audit report my office obtained, 18 individuals (including the Complainant) had their PIP profiles accessed by Dr. Haidash on January 24, 2009. Dr. Haidash's solicitor asserted that "January 24, 2009 was a Saturday and Dr. Haidash's clinic would not have been open. There would not have been any medical reason to access the profile." If this is true, then Dr. Haidash would not have had any medical reason to access any of the 18 PIP profiles that day. Therefore, 17 other individuals had their personal health information on PIP improperly accessed.

[27] The Complainant had only learned about Dr. Haidash's access to her PIP profile because she requested her PIP audit profile. However, if none of the 17 other individuals requested access to their own PIP audit report, then they may not be aware of how Dr. Haidash accessed their personal health information on PIP. What's also alarming is that Dr. Haidash's solicitor asserts that Dr. Haidash "picked unique names that he was familiar with" to train his wife on how to search a profile on PIP. This could suggest that Dr. Haidash accessed the personal health information of people he knows, including family, friends, foes, or acquaintances. Dr. Haidash's solicitor asserts that there is no evidence that any information was disseminated or accessed for any purpose other than training.

[28] My office's resource *Privacy Breach Guidelines for Trustees* recommends that trustees notify affected individuals when a privacy breach has occurred. Since these 17 other individuals have not been notified of Dr. Haidash's unauthorized access to their personal health information on PIP, then I find this privacy breach has not been dealt with adequately.

[29] Since Health is the trustee for PIP, my office will conduct an investigation into Health's role in this privacy breach. It will have further recommendations on how to deal with this matter.

III FINDINGS

[30] I find that HIPA is engaged.

[31] I find that section 26 does not authorize the use of personal health information for the purpose of training.

[32] I find that Dr. Haidash's access to the Complainant's personal health information on PIP was not in compliance with section 23 of HIPA.

[33] I find that Dr. Haidash was not in compliance with section 16 of HIPA at the time the Complainant's personal health information was accessed.

[34] I find that Dr. Haidash is still not in compliance with sections 16 and 23(2) of HIPA but he is taking appropriate steps to become compliant.

IV RECOMMENDATIONS

[35] I recommend that Dr. Haidash continue to develop written policies and procedures, as described in paragraphs [19] and [24], to be in compliance with subsections 16 and 23(2) of HIPA.

[36] I recommend that Dr. Haidash take into consideration my office's comments on the policies and procedures he is developing prior to finalizing them.

Dated at Regina, in the Province of Saskatchewan, this 28th day of March, 2017.

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